

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS**

A.D., C.A., R.G., T.B., E.W., M.H., and S.B.,
*individually and on behalf of all others similarly
situated,*

Plaintiffs,

v.

ASPEN DENTAL MANAGEMENT,
INC.,

Defendant.

Case No. _____

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs A.D., C.A., R.G., T.B., E.W., M.H., and S.B., individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby allege the following against Defendant Aspen Dental Management, Inc., a Delaware corporation (“Aspen,” “Aspen Dental” or “Defendant”). Facts pertaining to Plaintiffs and their experiences and circumstances are alleged based upon personal knowledge and all other facts herein are alleged based upon the investigation of counsel and, where indicated, upon information and good faith belief.

NATURE OF THE ACTION

1. Information concerning a person’s health is among the most confidential and sensitive information in our society and the mishandling of such information can have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.¹

¹ See, e.g., Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites*, potentially

2. Simply put, if people do not trust that their sensitive private medical information will be kept private and secure, they may be less likely to seek medical treatment which can lead to more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than authorized medical providers is vital to maintaining public trust in the healthcare system as a whole.

3. The need for data privacy, security and transparency is particularly acute when it comes to the rapidly expanding world of digital healthcare providers. Notably, of all the information the average internet user shares with technology companies, health data is some of the most extensive, valuable and controversial.²

Aspen Dental Collects a Significant Amount of Private Information via its Website.

4. The Aspen Group is a dental service organization that provides business support services to dentists, ranging from practice consulting to total practice management; Aspen proclaims that it brings numerous “centers of expertise,” like marketing, so that participating dentists can focus on delivering patient care.

endangering users in a post-Roe world, WIRED (Nov. 16, 2022), <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last visited Feb. 13, 2024).

² The highly sensitive medical information collected online includes many categories from intimate details of an individual’s conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. See Molly Osberg & Dhruv Mehrotra, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), available at <https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137> (last visited Feb. 13, 2024).

5. The Aspen Group’s Dental brand—Aspen Dental—has more than 900 locations across 48 states and the Aspen Dental network serves 35,000 patients a day—some as young as six years old.³

6. One of the services that Aspen provides, through Aspen Dental Management, Inc., is the maintenance of a website available at <https://www.aspendental.com/> (the “Site” or “Website”). Visitors to and users of the Site (“Users”) can search for information regarding the specific dental condition for which they are seeking treatment including (i) dentures (including information regarding replacement, repair and reline as well as cost); (ii) dental implants (including information regarding types of implants, cost and insurance options); (iii) emergency dental care (including root canals and tooth extraction); (iv) general dentistry services (checkups and teeth cleaning); (v) cosmetic dental procedures (including veneers, straightening and whitening); (vi) restoration services (including dental crowns and bridges as well as tooth filling) and (vii) oral surgery and periodontal disease treatment.⁴

7. The Site also allows Users to search for dentists based on proximity, their specific dental issues and/or treatments, as well as to make appointments for specific issues and/or treatments. As part of this process, a User provides numerous categories of personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “Private Information”) to Aspen. For instance, when a User navigates to the “Schedule an Appointment” page, the User is, first, required to provide information regarding the reason for their visit and, once selected, the subsequent pages prompt the User to provide a significant amount of Private

³ See <https://www.teamtag.com/our-story/> (last visited Feb. 13, 2024).

⁴ See <https://www.aspendental.com/dental-services/> (last visited Feb. 13, 2024).

Information including: (i) patient information (first and last name and date of birth); (ii) requested appointment information (including dentist, location, date and time) and (iii) additional patient information (including email, mobile phone number and whether the User has dental insurance).⁵

Aspen Dental Put Invisible Tracking Technologies on its Site.

8. The Users of Aspen's Site understandably thought that they were communicating *only* with their trusted healthcare provider but, in reality, Aspen installed tracking pixels and other technologies on its Site in order to collect and disclose confidential Private Information to third parties such as Facebook, Google (via Google Tag Manager, Google DoubleClick Ads, and Google Analytics), Bing, Salesforce and other marketing data brokers including AdRoll, Analyze.ly, AppNexus, Invoca, The Trade Desk and Qualtrics.

9. In fact, Aspen assured its Users in its Privacy Policy that it will use and disclose their health information only under certain circumstances such as "for treatment, payment and healthcare operations," ***none of which apply here.***⁶ Aspen further represented that unless a User

⁵ Additionally, through its Site, Aspen provides a number of patient services associated with the dental services sought by Users; for instance, Users can create accounts where they can manage appointments and pay bills as well as many other things. See <https://www.aspendental.com/patient-services> (last visited Feb. 13, 2024).

⁶ See Privacy Policy (Dec. 09, 2022), <https://web.archive.org/web/20221209120704/https://www.aspendental.com/privacy-policy/> (last visited Feb. 13, 2024). Aspen Dental changed its privacy policy sometime between December 09, 2022 and June 30, 2023, to disclose that it does, in fact, collect Users' protected personal information. See <https://www.aspendental.com/privacy-policy/> (last visited Feb. 13, 2024).

Further, while Aspen's responsibilities to protect patients' PHI should be explicitly covered by its Notice of Privacy Practices under HIPAA ("HIPAA Notice"), which must be posted on Aspen's Website, upon information and good faith belief Aspen failed to provide the HIPAA Notice to its patients and prospective patients online. See, e.g., <https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html> (last visited Feb. 14, 2024).

gives them “a written authorization, [Aspen] cannot use or disclose your health information for any reason except those described in this notice” and that it “will provide [the User] with notification of a breach of unsecured PHI as required by law.”⁷

10. Despite these representations, Aspen breached its own privacy policy by unlawfully intercepting and disclosing Users’ Private Information to Facebook, Google and likely other third parties without obtaining patients’ consent or authorization.

11. Invisible to the naked eye, pixels—which are configured by the website owner, here, Aspen—collect and transmit information from Users’ browsers to unauthorized third parties.

12. For instance, the Meta Pixel is a piece of code developed and licensed to website owners by Facebook (“Meta Pixel” or “Pixel”) that “tracks the people and [the] type of actions they take”⁸ as they interact with a website including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box), among many other things.

13. Together with the User’s Private Information, the data sent to Facebook also discloses their unique and persistent Facebook ID (“Facebook ID” or “FID”) which allows Facebook (and/or other third-parties) to specifically identify those Users and associate their Private Information with their Facebook profile.

14. Thus, in the case of information sent by Aspen to Facebook, the sensitive and protected Private Information is linked to Users’ unique Facebook IDs so that there is no

⁷ See Privacy Policy, *supra*, note 6.

⁸ Retargeting, <https://www.facebook.com/business/goals/retargeting> (last visited Feb. 13, 2024).

anonymity in that Facebook (and/or any third parties who access the information) are able to associate such personal health data with the specific User in question.

15. Aspen tracks, collects and divulges data even on people who do not have a Facebook account or have deactivated their Facebook accounts, and these individuals can find themselves in an even worse situation because when their Private Information is sent to Facebook, they cannot clear past activity or disconnect the collection of future activity since they do not have an account (or an active account).⁹

16. As Judge Orrick pointed out in a recent decision, non-Facebook Users who did not consent to Aspen's collection and disclosure of their data to Facebook (and other third party data brokers) are harmed in the same way as Users with active Facebook accounts in that "they paid more for their services from [their medical provider] than they otherwise would have had they know about Meta's interception of their information."¹⁰

17. Regardless of whether the User has a Facebook profile or not, Aspen transmits all of the Private Information collected by the Pixels—that *it* put on its Site—instantaneously and, perhaps needless to say, such collection and transmission is invisible and occurs without any notice to—and certainly no consent from—the Users.

⁹ See *Shadow profiles: Facebook has information you didn't hand over* (April 11, 2018), <https://www.cnet.com/news/privacy/shadow-profiles-facebook-has-information-you-didnt-hand-over/> (last visited Feb. 13, 2024).

¹⁰ See *E.H. & C.S. v. Meta Platforms, Inc.*, No. 23-cv-04784-WHO, Order on Mot. to Dismiss, at *7 (N.D. Ca. Feb. 12, 2024) (allowing non-Facebook users claims under the UCL and CLRA to proceed where plaintiffs alleged that Meta fraudulently omitted information about its collection of non-users' PHI, and plaintiffs alleged cognizable harm under "the benefit of the bargain theory.").

18. Upon information and good faith belief, Aspen also installed and implemented Facebook's Conversions Application Programming Interface ("Conversions API" or "CAPI") on its servers.¹¹

19. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to disclose information to third parties in addition to the website owner, CAPI does not cause the User's browser to transmit information directly to Facebook. Rather, CAPI tracks Users' Site interactions, including Private Information, records and stores that information on the Site owner's other workarounds such as ad blockers.¹²

20. By installing the Meta Pixel, CAPI, Google Tag Manager, Google Analytics and other tracking technologies including cookies and session replay, Aspen effectively planted "bugs" on its Users' web browsers and caused them to unknowingly disclose their private, sensitive and confidential health-related communications to Facebook and other unauthorized third party data brokers.

21. The decisions to use these tracking technologies were made by Aspen.

¹¹ While there is no way to confirm with certainty that a web host like Aspen has implemented Conversions API without access to the host server, companies like Facebook instruct web hosts to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Aspen "to share website events [with Facebook] that the pixel may lose." See *Best Practices for Conversions API*, META, <https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last visited Feb. 13, 2024).

¹² See <https://revealbot.com/blog/facebook-conversions-api/> (last visited Jan. 19, 2024). Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results." See <https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited Jan. 19, 2024).

22. The process of adding Pixels to the webpages on a given site is a multi-step process that must be undertaken by the website owner.¹³ In addition, website owners must agree to Facebook’s Business Tools Terms which require them to “represent and warrant” that they have prominently notified Users about the collection, sharing and use of data acquired by the Meta Pixel(s) on their Site(s).¹⁴

23. Aspen made the decisions to (i) use tracking technologies on its Site, (ii) use, specifically, the Meta Pixel and (iii) agree to Facebook’s Business Tools Terms for use of the Meta Pixel. In the process of doing so, Aspen decided to configure the Pixel to acquire as much Private Information as possible without Users’ informed consent.¹⁵

¹³ See *Business Help Center: How to set up and install a Meta Pixel*, <https://www.facebook.com/business/help/952192354843755?id=1205376682832142> (last visited Dec. 7, 2023); Ivan Mana, *How to Set Up & Install the Facebook Pixel (in 2022)*, <https://www.youtube.com/watch?v=ynTNs5FAUm8> (last visited Feb. 13, 2024); see also Colin Lecher & Ross Teixeira, *Facebook Watches Teens Online As They Prep For College*, THE MARKUP (Nov. 22, 2023), available at <https://themarkup.org/pixel-hunt/2023/11/22/facebook-watches-teens-online-as-they-prep-for-college> (stating that “[b]usinesses embed the pixel on their own websites voluntarily, to gather enough information on their customers so they can advertise to them later on Meta’s social platforms”) (last visited Feb. 13, 2024).

¹⁴ See *Meta Business Tools Terms*, https://www.facebook.com/legal/businesses/paipv=0&eav=AfbOvnb7E0sZ-wzgCW6xNLFKEOEvh_fr6JjkMINTJNqN7i1R-3MPh5caFgmdgAOxbL8&_rdr (requiring companies to agree that they will not share, among other things, sensitive health information.) (last visited Feb. 13, 2024); see also Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report*, NEWSBYTES (June 16, 2022) <https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story> (quoting Facebook spokesman Dale Hogan as saying that it is “against [Facebook’s] policies for websites and apps to send sensitive health data about people through [its] Business Tools”) (last visited Feb. 13, 2024).

¹⁵ The Pixels are configurable by the end-user such that once a webpage containing a pixel is loaded onto a user’s web browser, the Pixel uses the snippet of code to connect to Facebook servers, which contain the bulk of the Pixel’s actual programming. Once fully loaded and operational, the Pixel prompts the user’s web browser to transmit specific information based on parameters set by the website owner. This customizable nature of the Meta Pixel allows the website

24. Moreover, Aspen’s overall intent and purpose in acquiring Users’ personal health data was to increase its ability to market and retarget its Users, thereby increasing its profit while violating HIPAA, state and federal statutes, and common law.

25. While this Complaint primarily focuses on how Aspen configured the Meta Pixel on its Site to collect and disclose Users’ Private Information, other tracking technologies embedded by Aspen—such as Google, Bing, AdRoll, analyze.ly and Qualtrics tracking codes—also collect Private Information, and the respective tech companies have the capability to link it to specific user profiles they maintain.¹⁶

26. Then, completely unencumbered by any pretense of restriction or regulation, these third-party platforms, in turn, use that Private Information for various business purposes including using such information to “improve” advertisers’ ability to target specific demographics and selling such information to third-party marketers who target those Users online (*i.e.*, through their Facebook, Instagram, Gmail and other social media and personal accounts).¹⁷

owner to determine which webpages contain the Pixel, which events are tracked and shared with Facebook and whether these events are classified as standard or custom events.

¹⁶ For example, Google stores Users’ logged-in identifier on a non-Google website in its logs. Whenever a User logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the User’s browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads.

¹⁷ See Lecher & Teixeira, *supra*, note 13 (“Along with encouraging businesses to spend ad dollars, Facebook also receives the transmitted data, and can use it to hone its algorithms. Facebook can also use data from the pixel to link website visitors to their Facebook accounts, meaning businesses can reach the exact people who visited their sites. The pixel collects data regardless of whether the visitor has an account.”).

Aspen Derives Significant Value from Users' Valuable Private Information.

27. These third parties are not the only entities that use and monetize Users' Private Information collected without their consent as Aspen itself directly benefits by using the data it surreptitiously collects.

28. While the information captured and disclosed without permission may vary depending on the pixel(s) embedded, the "data packets" can be extensive in that they collect and transmit the contents of Users' communications and numerous other pieces of information including, but not limited to: (i) the User's first and last name, (ii) the User's date of birth; (iii) the User's email address, phone number and other personal information; (iv) when a User accesses the Site; (v) the exact text of the User's search queries; (vi) medical services and treatments sought; (vii) scheduling of appointments; (viii) accessing and viewing account information; (ix) the text of URLs visited by the User and (x) other information that qualifies as PII and PHI under federal and state laws.

29. The data in the "data packets" is then linked to the User's unique Facebook ID and their specific internet protocol ("IP") address, which is itself protected information under the Health Insurance Portability and Accountability Act ("HIPAA").¹⁸

¹⁸ The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual. These HIPAA Identifiers, as relevant here, include names, dates related to an individual, email addresses, device identifiers, web URLs and IP addresses. *See Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule ("HHS Guidance Regarding Methods for De-identification of PHI")*, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Feb. 13, 2024).

30. The information intercepted by the Pixels and third-party tracking technologies is used to build incredibly fulsome and robust marketing profiles for individual Users and create targeted advertisements based on the medical conditions and other Private Information disclosed. Despite the clear and unequivocal prohibition on the disclosure of PHI without consent, Aspen chose to use the Pixel and CAPI data for marketing purposes to bolster its revenue.

31. The reason that Aspen went to these lengths to obtain this sensitive Private Information is, quite simply, because its patients would *not* provide it if they were informed and given a choice. That is, if Aspen informed its Users that by using its Site their sensitive Private Information would be collected and disseminated to Facebook and/or other third-party platforms for marketing and analytics purposes (among others), those Users would understandably not consent or they would demand significant compensation for the use of their private and valuable health information in this manner.

32. Thus, by deciding to use pixels (and other third-party tracking technologies) to collect Users' Private Information, Aspen was unjustly enriched in that it acquired highly sensitive information that it would not be able to obtain otherwise or for which it would have to pay significantly.

33. Aspen also uses this impermissibly obtained data for analytics purposes to gain additional insights into how its patients use its Site.¹⁹

¹⁹ While gaining additional insights into its User base is not a bad thing necessarily, Aspen unquestionably was required to inform its Users that it had deployed tracking technologies on its Site so that those Users could make an informed decision as to whether they wanted their information to be collected, disclosed and used in this manner. The OCR Bulletin discussed herein is instructive: "disclosures of PHI to tracking technology vendors for marketing purposes, *without individuals' HIPAA-compliant authorizations*, would constitute impermissible disclosures." See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>

Aspen's Disclosure of Users' Private Information Without Consent Violates the Law.

34. Users of Aspen's Site thought they were communicating *only* with their trusted healthcare providers. But by employing third-party trackers—which obtain detailed data concerning its patients' medical information—Aspen effectively bartered their Private Information for more detailed analytics of its Users to increase its revenues and profits.

35. Healthcare patients simply do not anticipate that their trusted healthcare provider will send Private Information collected via its web pages to an undisclosed third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without their informed and express consent.²⁰

36. Simply put (and as detailed herein), covered entities such as Aspen are *not* permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third-party without express and informed consent from each patient.

37. As recognized by both the Federal Trade Commission ("FTC") and the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS"), healthcare companies' use of tracking technologies to collect and divulge their patients' sensitive and confidential information is an extremely serious data security and privacy issue:

In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. **But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by**

("OCR Bulletin") (emphasis added) (last visited Feb. 13, 2024).

²⁰ This Court will not have to look far to find evidence of Meta's violations of privacy laws. In May of last year, for example, the European Union fined Meta "a record-breaking" \$1.3 billion for violating EU privacy laws. See Hanna Ziady, *Meta slapped with record \$1.3 billion EU fine over data privacy*, <https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html> (last accessed Feb. 13, 2024).

*sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.*²¹

38. Similarly, OCR is clear that “[r]egulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.”²²

39. This is precisely the conduct that Aspen is engaging in, as these tracking codes are *not* required for Aspen’s Site to operate; instead, they collect data that is later used for marketing, remarketing and advertising purposes by Aspen and third parties to whom it is disclosed.

40. The facts of this unauthorized interception of Plaintiffs’ Private Information are overwhelmingly offensive; as noted by the Honorable William Orrick in a case pending against Facebook’s parent company concerning the use of Pixel tracking on hospital websites, consumers “would be shocked” to learn of the scope and nature of the information collected.²³

²¹ See Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023) (emphasis added), available at <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases> (last visited Feb. 13, 2024).

The FTC is walking the walk with respect to health companies’ use of tracking technologies in this fashion. For example, as a result of a recent FTC enforcement action, GoodRx agreed to pay a \$1.5 million civil penalty for failing to report its unauthorized disclosure of consumer health data to Facebook, Google and other companies. See, e.g., Todd Feathers, THE MARKUP, *The FTC Is Taking on Telehealth’s Data Sharing Problem—Starting with GoodRx*, (Feb. 1, 2023) (“In a ‘first-of-its-kind’ action with broad implications for the telehealth industry, the Federal Trade Commission on Wednesday sought a court order to prevent GoodRx, a popular website that provides discounts on prescription drugs, from sharing users’ sensitive health data for advertising purposes.”), available at <https://themarkup.org/pixel-hunt/2023/02/01/the-ftc-is-taking-on-telehealths-data-sharing-problem-starting-with-goodrx> (last visited Feb. 13, 2024).

²² OCR Bulletin, *supra*, note 19 (emphasis added).

²³ See *Doe v. Meta Platforms Inc.* (N.D. Cal., No. 3:2022cv03580) ECF No. 141; see also <https://www.law360.com/articles/1548383/facebook-health-tracking-claim-shocking-if-true->

41. Aspen's obligation to protect and secure the Private Information entrusted to it is **not** new as the OCR recently **reminded** HIPAA-regulated entities, in its *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* bulletin that such tracking and disclosures are **not** permitted under HIPAA.

42. While healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, they can do so only in a very limited way:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... ***If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.***²⁴

43. Despite numerous warnings from federal regulators (not to mention several FTC enforcement actions against telehealth companies for similar conduct) about the data privacy risks of using third-party tracking technologies,²⁵ Aspen put various tracking technologies on its Site in order to acquire and transmit Users' Private Information without their informed consent.

judge-says. Indeed, the HHS Bulletin noted that "because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI [personal health information] **only** as expressly permitted or required by the HIPAA Privacy Rule."

²⁴ See *HHS Guidance Regarding Methods for De-identification of PHI*, *supra*, note 18 (noting that "HIPAA Identifiers" include name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

²⁵ See, e.g., Heather Landi, *Regulators Warn Hospitals and Telehealth Companies about privacy*

44. Aspen further made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that Users exchanged with Aspen.

45. As detailed herein, Aspen owed common law, statutory and regulatory duties to keep its Users' Private Information safe, secure and confidential. Aspen breached those duties and obligations by, *inter alia*: (i) failing to adequately review its marketing programs to ensure its Site was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Users' Private Information; (iii) failing to obtain the prior written consent of Users to disclose their Private Information to Facebook and/or others before doing so; (iv) failing to take steps to block the transmission of Users' Private Information through Meta Pixels and other tracking codes; (v) failing to warn Users that their Private Information was being shared with third parties without express consent and (vi) otherwise failing to design and monitor its Site to maintain the security, confidentiality and integrity of patient Private Information.

Aspen Has Not Informed Users of Its Use of Tracking Technologies on its Site.

46. Despite incorporating the Meta Pixel (and other tracking technologies) into its Site and servers, Aspen has—to this day—not disclosed to Users that it divulged their sensitive and confidential Private Information with Facebook.

risks of Meta, Google Tracking Tech (July 21, 2023), <https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google> (noting that the FTC and the OCR issued a rare joint release announcing that 130 hospital systems and telehealth providers received a letter warning them about the data privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps) (last visited Feb. 13, 2024).

47. In recent months and in stark contrast to Aspen, several medical providers that used the Meta Pixel in a similar way have provided their patients with notice that their Private Information was transmitted to third parties.²⁶

48. Here, not only has Aspen declined to report its (virtually identical) unauthorized disclosures, but it also—even *after receipt of Plaintiff's demand letter in April of last year*—continues to disclose Users' Private Information to third parties through Google Tag Manager, Google Analytics, Google DoubleClick Ads, Bing Universal Event Tracking, Salesforce Marketing Personalization (Evergage), Invoca, Qualtrics, AdRoll, AppNexus, Analyze.ly Connect and The Trade Desk.

49. At least the following trackers on Aspen's Site are disclosing the Users' search queries: Google Tag Manager, Google DoubleClick Ads and Google Analytics.

Aspen's Conduct Caused Concrete & Demonstrable Harm to Users.

50. Aspen's decisions to prioritize its own revenues and profits over the privacy rights of its Users has serious, real-world consequences; indeed, as noted by the OCR Bulletin, "[a]n impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, **discrimination, stigma,**

²⁶ See, e.g., *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Feb. 13, 2024); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3> (last visited Feb. 13, 2024); *Novant Health notifies 1.36 Million Patients About Unauthorized Disclosure of PHI via Meta Pixel Code on Patient Portal* (Aug. 16, 2022), <https://www.hipaajournal.com/novant-health-notifies-patients-about-unauthorized-disclosure-of-phi-via-meta-pixel-code-on-patient-portal/> (last visited Feb. 13, 2024).

mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, *including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.* While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, *because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*"²⁷

51. Users of the Site have suffered injury because of Aspen's unlawful and outrageous conduct; these injuries include: (i) invasion of privacy, (ii) loss of benefit of the bargain, (iii) compromise and disclosure of Private Information, (iv) diminution of value of their Private Information, (v) statutory damages and (vi) the continued and ongoing risk to their Private Information.²⁸

52. Plaintiffs, on behalf of themselves and all similarly situated individuals, seek to remedy these harms and assert individual and representative claims against Aspen for: (i) Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq.* (the "ECPA"), Unauthorized Interception, Use and Disclosure; (ii) Negligence; (iii) Common Law Invasion of Privacy – Intrusion Upon Seclusion; (iv) Unjust Enrichment; (v) Breach of Implied Contract; (vi) Violation of Illinois Consumer Fraud and Deceptive Business Practices Act; (vii) Violation of

²⁷ OCR Bulletin, *supra*, note 19 (emphasis added).

²⁸ The exposed Private Information of Users can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties often offer for sale the unencrypted, unredacted Private Information to criminals on the dark web for use in fraud and cyber-crimes.

Illinois Eavesdropping Statute; (viii) Violation of the Florida Security of Communications Act (“FSCA”), Fla. Stat. 934.01, *et seq.*; (ix) Violation of the Massachusetts Consumer Protection Act, M.G.L. § 93A *et seq.*; (x) Violation of the Massachusetts Wiretap Act, M.G.L. c. 272 § 99; (xi) Violation of the Washington Consumer Protection Act, Wash. Rev. Code Ann. §§ 19.86.020, *et seq.*; (xii) Violation of the Washington Health Care Information Act (“HCIA”), RCW 70.2.005, *et seq.*; and (xiii) Identity Theft in Violation of RCW 9.35.020.

PARTIES

A. The Representative Plaintiffs

53. Plaintiff A.D. is a resident of Cook County, Illinois and used the Aspen Site while in Illinois.

54. Plaintiff C.A. is a resident of Cook County, Illinois and used the Aspen Site while in Illinois.

55. Plaintiff R.G. is a resident of Marion County, Illinois and used the Aspen Site while in Illinois.

56. Plaintiff T.B. is a resident of Chittenden County, Vermont and used the Aspen Site while in Vermont.

57. Plaintiff E.W. is a resident of Spokane County, Washington and used the Aspen Site while in Washington.

58. Plaintiff M.H. is a resident of Washington County, Florida and used the Aspen Site while in Florida.

59. Plaintiff S.B. is a resident of Worcester County, Massachusetts and used the Aspen Site while in Massachusetts.

60. Plaintiffs are long-time patients of Aspen and have visited and used the Aspen Site to make appointments in the past two years.

61. Plaintiffs each viewed and interacted with numerous pages on the Site including, but not limited to, researching and reviewing dental procedures and issues for which they were considering seeking dental treatment.

62. Plaintiffs understandably and reasonably believed and trusted that their Private Information provided to Aspen via the Site would be kept confidential and secure and would be used solely for authorized purposes.

B. Defendant Aspen Dental Management, Inc.

63. Aspen Dental Management, Inc. is an American dental support organization incorporated in Delaware and headquartered at 806 W. Fulton Market in Chicago, Illinois 60607.

JURISDICTION & VENUE

64. This Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this Complaint asserts a claim for violation of federal law, specifically, the ECPA, 18 U.S.C. § 2511. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

65. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

66. This Court has personal jurisdiction over Aspen because it operates and maintains its principal place of business in this District. Further, Aspen is authorized to and regularly conduct business in this District and make decisions regarding corporate governance and management of the Website in this District, including decisions regarding the privacy of User's Private Information and the incorporation of the Pixels and other tracking technologies.

67. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including decisions made by Aspen's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiffs' and Class Members' Private Information; Aspen's principal place of business is located in this District; Aspen collects and redistributes Class Members' Private Information thereby causing harm to Class Members residing in this District.

COMMON FACTUAL ALLEGATIONS

A. Federal Regulators Make Clear that the Use of Tracking Technologies to Collect & Divulge Private Information Without Informed Consent is Illegal.

68. This surreptitious collection and divulgence of Private Information is an extremely serious data security and privacy issue. Both the Federal Trade Commission and the Office for Civil Rights of the Department of Health and Human Services ("HHS") have, in recent months, reiterated the importance of and necessity for data security and privacy concerning health information.

69. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health.*** Indeed, [recent

FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning ‘pregnancy mode’ on or off) may itself be health information.***”²⁹

70. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

Don’t use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.

In today’s surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. **But when companies use consumers’ sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.**

[Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that **may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers’ affirmative express consent for the disclosure of sensitive health information.**³⁰

²⁹ *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases, supra*, note 21.

³⁰ *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers’ authorization.

71. The federal government is taking these violations of health data privacy and security seriously as shown by the recent high-profile FTC settlements against several telehealth companies.

72. For example, earlier this year the FTC imposed a \$1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and platforms including Facebook, Google and Criteo, and proposed a \$7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Facebook and Snapchat for advertising purposes. And Easy Healthcare was ordered to pay a \$100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app Premon shared health data for advertising purposes.³¹

73. Even more recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about the use of online tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the "risks and concerns about the use of technologies, such as the Meta/Meta Pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures

³¹ See Jill McKeon, *How FTC Enforcement Actions Will Impact Telehealth Data Privacy*, <https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy>; see also Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), www.law360.com/articles/1571369/ftc-targets-goodrx-in-1st-action-under-health-breach-rule?copied=1 ("The Federal Trade Commission signaled it won't hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale."); <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising>; <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premon-will-be-barred-sharing-health-data-advertising-under-proposed-ftc> (last visited Feb. 14, 2024).

of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others." According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."³²

74. Moreover, the OCR has made clear that the transmission of such protected information violates HIPAA's Privacy Rule:

75. "Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. *For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.*"³³

76. The OCR Bulletin reminds healthcare organizations regulated under HIPAA that they may use third-party *tracking* tools, such as Google Analytics or Meta Pixels *only in a limited way*, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.³⁴

77. The OCR Bulletin further discusses the harms that disclosure may cause patients:

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss,

³² OCR Bulletin, *supra*, note 19.

³³ *Id.* (emphasis added).

³⁴ *See id.*

discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, *including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.* While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, *because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*³⁵

78. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to monetize their users' Private Information. For instance, THE MARKUP reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.³⁶

79. And, in the aptly titled report "*Out of Control*": *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and The Markup of 50 direct-to-consumer telehealth companies, reported that telehealth companies or virtual care websites were providing sensitive medical information they collect to the world's largest advertising platforms.³⁷

³⁵ *Id.* (emphasis added).

³⁶ See Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP, <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited Feb. 13, 2024).

³⁷ Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, "*Out Of Control*": *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation*

80. Many telehealth sites had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn and/or Pinterest—that collected patients’ answers to medical intake questions.³⁸

B. The Tracking Pixel.

81. A “pixel” is a piece of code that “tracks the people and the types of actions they take”³⁹ as they interact with a website, including how long a person spends on a particular webpage, which buttons the person clicks, which pages they view, the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), and more.

82. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting—*i.e.*, serving online advertisements to people who have previously engaged with a business’s website—and other marketing.

83. Here, a User’s web browser executes the Pixels via instructions within each webpage of Aspen’s Site to communicate certain information – within parameters set by Defendant – directly to Facebook, Google and other third party Pixel data recipients (such as, for example, Salesforce, Invoca, and Qualtrics which can collect data from the Meta Pixel) .

by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech’s tracking tools (Dec. 13, 2022), <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies> (last visited Feb. 13, 2024).

³⁸ *See id.* (noting that “[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan”).

³⁹ *Retargeting*, <https://www.facebook.com/business/goals/retargeting> (last visited Feb. 13, 2024).

84. The Pixels can also share the User's identifying information for easy tracking via the "cookies"⁴⁰ stored on their computer by Facebook and/or Google.

85. For example, Facebook stores or updates Facebook-specific cookies every time a person accesses their Facebook account from the same web browser. The Meta Pixel can access these cookies and send certain identifying information like the user's Facebook ID (represented by the value of Facebook's "c_user" cookie) to Facebook along with the other data relating to the user's Website inputs.

86. The same is true for the other Pixel data recipients, which also create cookies that are stored in the user's computer and accessed by the pixels (and other tracking codes) to identify the user. Google, Bing and other data brokers likewise process this data in a similar manner and use it to connect the information to particular individuals to build marketing and other data profiles.

87. The Pixels and other tracking codes are programmable, meaning that Defendant controls which of the webpages on the Website contain the codes, and which events are tracked and transmitted to Facebook, Google, and other third parties.

88. Aspen embedded several tracking codes on its Site, which secretly recorded and transmitted patients' Private Information to third parties including Facebook, Google, Bing, Salesforce and other marketing data brokers.

89. Once put on the Site *by Aspen* and configured *by Aspen*, these tracking technologies (including the Pixel) operated as a wiretap, silently monitoring User activity on those webpages

⁴⁰ "Cookies are small files of information that a web server generates and sends to a web browser. Cookies help inform websites about the user, enabling the websites to personalize the user experience." See *What are cookies?/ Cookies definition*, <https://www.cloudflare.com/learning/privacy/what-are-cookies/> (last visited Feb. 13, 2024).

and intercepting the Private Information that Users sent via the Site to Aspen and transmitting that Private Information directly to third parties (like Facebook) without the required informed consent.

90. Aspen configured the Meta Pixel to track Users on its Site as early as January 2016 and continued disclosing Users' Private Information to Facebook until at least September 6, 2023.

91. Through this tracking, Aspen disclosed to Facebook (i) when Users viewed Aspen's locations and services, (ii) Users' search activities, (iii) services and/or treatments sought by each User; (iv) Users' locations and (v) when Users scheduled appointments.

92. And, *even after receipt of a demand letter from Plaintiff T.B. in April of 2023*, Aspen continues to disclose Users' Private Information to third parties through Google Tag Manager, Google Analytics, Bing Universal Event Tracking, Salesforce, Invoca, Qualtrics, AppNexus, Analyze.ly Connect and The Trade Desk.

93. Defendant used the data it collected from Plaintiffs and Class Members, without their consent, to improve its advertising and bolster its revenues.

C. Facebook Uses Certain "Business Tools" to Match the Information It Collects To Facebook Users.

94. Facebook operates the world's largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.⁴¹

95. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target and market products and services to individuals.

⁴¹ META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Feb. 13, 2024).

96. Facebook’s Business Tools, including the Meta Pixel, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

97. The Business Tools are automatically configured to capture “Standard Events” such as when a user visits a particular webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, button clicks, etc.⁴²

98. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a “custom event.”⁴³

99. One such Business Tool is the Meta Pixel, which “tracks the people and type of actions they take.”⁴⁴

100. When a user accesses a webpage that is hosting the Meta Pixel, like Defendant’s Website, their communications with the host webpage are instantaneously and surreptitiously

⁴² *Specifications for Facebook Pixel Standard Events*, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142> (last visited Feb. 13, 2024).; *see*, META PIXEL, GUIDES, ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/> (last visited Feb. 13, 2024).; *see also* BEST PRACTICES FOR META PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142> (last visited Feb. 13, 2024).; META MARKETING API, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Feb. 13, 2024).

⁴³ ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142> (last visited Feb. 13, 2024).; *see also* META MARKETING API, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Feb. 13, 2024).

⁴⁴ RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Feb. 13, 2024).

duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

101. This secret transmission to Facebook contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code and Facebook's embedded code.

102. Accordingly, during the same transmissions, the Website code routinely provides Facebook with Defendant's patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into the Website, including not only their medical searches, treatment requests, and the webpages they view, but also their name, gender, email address, phone number, city and zip code . This is precisely the type of identifying information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.⁴⁵

103. Plaintiffs' and Class Members' identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

104. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. When the Website visitor is also a Facebook user, the information collected via the Meta Pixel is associated with the User's Facebook ID that identifies their name and Facebook profile, *i.e.*, their real-world identity.

⁴⁵ <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Feb. 13, 2024).

105. Importantly, Facebook maintains “shadow profiles” on users without Facebook accounts and links the information collected via the Meta Pixel to the user’s real-world identity using their shadow profile.⁴⁶

106. The Private Information disclosed via the Pixel allows Facebook to know that a specific User is seeking confidential medical care and the type of medical care being sought. Facebook then uses that information to sell advertising to Defendant and other advertisers and/or sells that information to marketers who will online target Plaintiffs and Class members.

107. With substantial work and technical know-how, internet users can sometimes circumvent the browser-based wiretap technology of the Pixels. This is why third parties determined to gather Private Information, like Facebook, implement workarounds that even savvy users cannot evade, discussed *infra*.

108. The third parties to whom a website transmits data through pixels and associated workarounds track user data and communications for their own marketing purposes, and for the marketing purposes of the website owner. Ultimately, the purpose of collecting user data is to make money.

109. Thus, without any knowledge, authorization, or action by a user, website owners like Defendant use source code to commandeer the User’s computing device, causing the device to contemporaneously and invisibly re-direct the Users’ communications to third parties.

⁴⁶ See Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook’s Privacy Defense*, TheVerge.com (Apr 11, 2018), available at <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy> (last visited Feb. 13, 2024).

110. In this case, Defendant employed the Pixels and other tracking technologies, to intercept, duplicate, and re-direct Plaintiffs' and Class members' Private Information to Facebook, Google and the other Pixel data recipients.

111. In sum, the Pixels and other tracking technologies on the Website transmitted Plaintiffs' and Class members' highly sensitive communications and Private Information to Facebook and Google (as well as other Pixel data recipients), which communications contained private and confidential medical information. These transmissions were performed without Plaintiffs' or Class members' knowledge, consent, or express written authorization.

D. Facebook Uses Unique Identifiers to Match the Information It Collects With Facebook Users

112. Facebook uses cookies to identify Users, including cookies named c_user, datr, fr, and _fbp. Facebook stores or updates Facebook-specific cookies every time a person accesses their Facebook account from the same web browser.

113. The Meta Pixel can access these cookies and send certain identifying information like the user's Facebook ID to Facebook along with the other data relating to the user's website inputs.⁴⁷

114. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.⁴⁸

⁴⁷ The same is true for Google and other Pixel data recipients, which also create cookies that are stored in the user's device and accessed by the Pixels to identify the user.

⁴⁸ An unskilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse, (3) selecting "View page source," (4) executing a control-f function for "UserID," and (5) copying the number value that appears after "UserID" in the page source code of the Facebook user's page.

115. A User's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the User's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

116. The Facebook datr cookie identifies the User's web browser. It is an identifier unique to each person's specific web browser, and is another way Facebook can identify Facebook users.

117. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Meta by using the Facebook "Download Your Information" tool.

118. The Facebook fr cookie is an encrypted combination of the c_user and datr cookies.⁴⁹

119. The c_user, datr, and fr cookies are traditional third-party cookies, meaning they are cookies associated with a party other than the entity with which a person is communicating at

Following these directions makes it possible to discover that the Facebook UserID assigned to Mark Zuckerberg is 4. By typing www.facebook.com/4 into a browser and hitting enter, a browser directs to Mr. Zuckerberg's page at www.facebook.com/zuck.

⁴⁹ See Gunes Acar, et al., *Facebook Tracking Through Social Plug-ins: Technical Report Prepared for the Belgian Privacy Commission* (Mar. 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

the time. In the case of Piedmont, they are third-party cookies because Meta is a third-party to the communication between a patient and their healthcare provider.

120. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the healthcare provider using the Facebook Pixel.

121. The fbp cookie is also a third-party cookie in that it is also a cookie associated with Facebook that is used by Facebook to associate information about a person and their communications with non-Facebook entities while the person is on a non-Meta website or application, i.e. it is also used by Facebook as a personal identifier to match the “event” captured on a website to a particular Facebook user.

122. Facebook disguises the _fbp cookie as a first-party cookie even though it is Facebook’s cookie on non- Facebook websites.

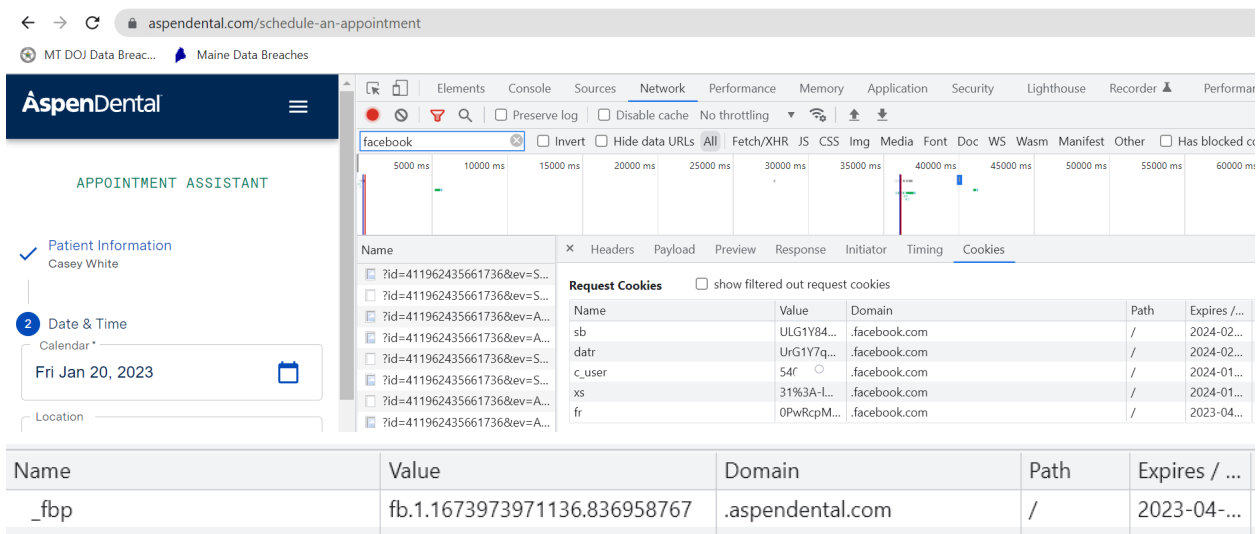
123. By disguising the _fbp cookie as a first-party cookie for a healthcare provider rather than a third-party cookie associated with Facebook, Facebook ensures that the _fbp cookie is placed on the computing device of Users who seek to access the Website but use third-party cookie blockers.

124. The _fbp cookie is then used as a unique identifier for that User by Facebook. If a User takes an action to delete or clear third-party cookies from their device, the _fbp cookie is not impacted – even though it is a Facebook cookie – again, because Facebook has disguised it as a first-party cookie.⁵⁰ Facebook also uses IP address and user-agent information to match the health information it collects from Facebook healthcare partners with Facebook users.

⁵⁰ Upon information and good faith belief, the __ga and _gid cookies operate similarly as to Google.

125. Defendant deposits cookies used by Facebook (and/or Google) to identify individuals, including those named `_fbp`, `datr`, `fr`, `c_user`, `_ga` and `_gid` on its Users' computing devices.

Figures 1-2. Examples of Facebook cookies on Aspen's Website:



E. Conversions API.

126. Facebook Conversions API and similar tracking technologies allow businesses to send web events, such as clicks, form submissions, keystroke events and other user actions performed by the user on the Website, from their own servers to Facebook and other third parties.⁵¹

127. Conversions API creates a direct and reliable connection between marketing data (such as website events and offline conversations) from Aspen's server to Facebook.⁵² In doing

⁵¹ See <https://revealbot.com/blog/facebook-conversions-api/> (last visited Feb. 13, 2024).

⁵² See <https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited Feb. 13, 2024).

so, Aspen stores Plaintiffs' and Class Members' Private Information on its own server and then transmits it to unauthorized third parties.

128. Conversions API is an alternative method of tracking versus the Meta Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side" implementation of tracking technology whereas the Pixels are "client-side," *i.e.*, executed on users' computers in their web browsers.

129. Because Conversions API is server-side, it cannot access the Facebook `c_user` cookie to retrieve the User's Facebook ID.⁵³ Therefore, other roundabout methods of linking the user to their Facebook account are employed.⁵⁴

130. For example, Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Meta Pixel and Conversions API are executed.⁵⁵

131. Conversions API tracks the user's website interaction, including Private Information being shared, and then transmits this data to Facebook and other third parties. Facebook markets Conversions API as a "better measure [of] ad performance and attribution

⁵³ "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses and phone numbers, that we use for matching purposes only." See <https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/> (last visited Feb. 13, 2024).

⁵⁴ "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." <https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req-rec-params> (last visited Feb. 13, 2024).

⁵⁵ See <https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events> (last visited Feb. 13, 2024).

across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results.”⁵⁶

132. Aspen installed the Pixels and, upon information and good faith belief, Conversion API, as well as other tracking technologies on many (if not all) of the webpages within the Website and programmed or permitted those webpages to surreptitiously share Users' Private Information with Facebook and Google (as well as other Pixel data recipients)—communications that included Plaintiffs' and Class Members' Private Information.

F. Aspen's Use of the Pixel to Transmit Users' Private Information to Unauthorized Third Parties Such As Facebook.

133. When Users visit Defendant's Site via an HTTP Request to Aspen's server, Defendant's server sends an HTTP Response, including the Markup that displays the Webpage visible to the user and Source Code (with the Pixel).

134. The User visiting this web page only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

135. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and to send those communications to Facebook, including full string URLs containing terms entered into search fields and fillable forms, button click data and keystrokes.

136. This occurs because the Pixel embedded in Aspen's Source Code is programmed to automatically track and transmit Users' communications contemporaneously, invisibly and without patient knowledge.

⁵⁶

About *Conversions*
<https://www.facebook.com/business/help/2041148702652965?id=818859032317965>
 visited Feb. 13, 2024).

API,
 (last

137. Thus, without consent, Defendant has effectively used its source code to commandeer patients' computing devices, thereby re-directing their Private Information to third parties.

138. Aspen configured a Meta Pixel (ID number 411962435661736) to track Users on its Site as early as January 2016 and continued disclosing Users' Private Information to Facebook until at least September 6, 2023.

139. Aspen also discloses Users' Private Information to third parties through Google Tag Manager, Google Analytics, Bing Universal Event Tracking, Salesforce, Invoca, Qualtrics, AppNexus, Analyze.ly Connect and The Trade Desk.

140. Aspen configured the Pixel to enable the collection of information about "standard events" such as "PageView" (which tells Facebook the URLs of web pages visited by Users), "Microdata" (includes information like the page's title and description) and "SubscribedButtonClick" (which tracks clicks on buttons; the information sent to Facebook includes the button's inner text). Information sent to Facebook by the Pixel included which Users were searching for a specific treatment, looking at pricing for a specific treatment or scheduling an appointment at a specific location for a specific treatment sought.

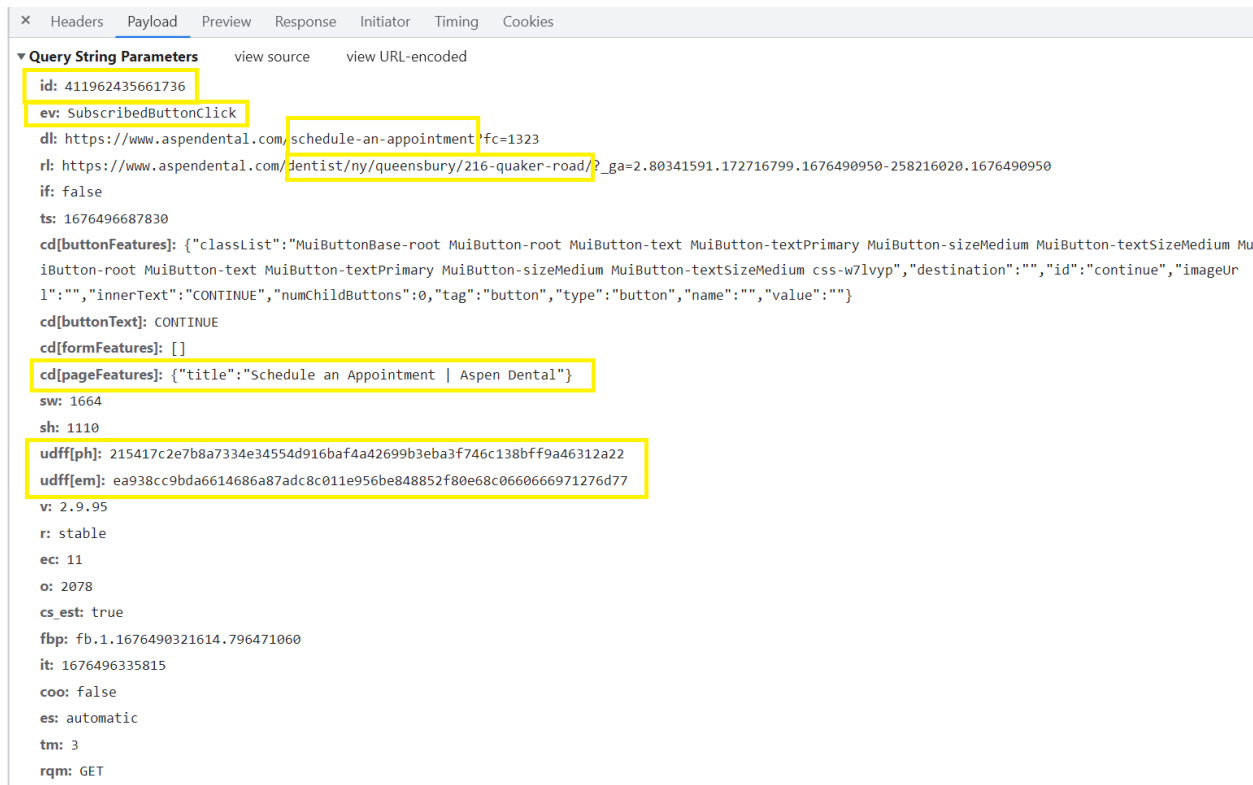
Figure 3. Example of the Pixel's operation on the Website - an HTTP single communication session sent from the device to Facebook that reveals that the User is scheduling an appointment after selecting a specific treatment for the visit, along with the User's unique Facebook personal identifier (the c_user field):

```
Rquest Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?id=411962435661736&ev=SubscribedButtonClick&l=https%3A2F2Fwww.aspendental.com% schedule-an-appointment rl=https%3A2F2Fwww.aspendental.com%2Fsched
ule-an-appointment&if=false&ts=1673974066111&cId%5BbuttonFeatures%5D=%7B%22classList%2%3A%22MuiButtonBase-root%20MuiToggleButton-root%20MuiToggleButton-sizeMediu
m%20MuiToggleButton-standard%2 reasonForVisitButton%20css-rmClcf%22%2C%22destination%22%3A%22%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3
A% Dentures %22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22button%22%2C%22type%22%3A%22button%22%2C%22name%22%3A%22%22%2C%22value%22%3A%22%22%7D&cId%5BbuttonText
%5D=Dentures&cId%5BFormFeatures%5D=%7B%22cId%5BpageFeatures%5D=%7B%22title%22%3A%22Schedule%20an%20Appointment%20%7C%20Aspen%20Dental%22%7D&cId%5Bparameters%5D=%
B%5D&sw=1664&sh=11108&v=2.9.92&r=stable&ec=2&o=30&fbp=fb.1.1673973971136.836958767&it=16739739960558coo=false&es=automatic&t=3&rqm=GET&d=hmgriizl9l8l6duom15be525
k87cydwh
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
cookie: sb=ULGIY84MPlrt6SjYXlhfavO; datr=UrgIY7qnkrzIH6f4IXAXVKPw; C_user=540 ; xs=31%3A-lQFI1sbXN5KM-g%3A2%3A1673409765%3A-1%3A3037; fr=0PwRcpMYRX9fv1Tnb.AWw
hc3yHtDt4DLK7L7ntib3OKGA.BjtbfQ.-H.AAA.0.0.bvjvtK.AwwHH6nz4-I
referer: https://www.aspendental.com/
```

141. The Pixel also collected information about “customized events” such as “InferredEvents,” “Microdata,” “AutomaticMatching,” “OnlineAppointment,” “Schedule Combined” and “AutomaticSetup.”

142. The AutomaticMatching was configured to match—among other PII—the User’s (hashed) email, first and last name, (hashed) phone number, gender, city and zip code, entered on the Site, to the considerable information Facebook has on that User.

Figure 4: Example of Aspen’s embedded Pixel collecting and sharing information that the User is scheduling an appointment at a specific location, along with their hashed phone number and email (“udff” fields):⁵⁷



143. While the Meta Pixel tool “hashes” personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent Facebook from reading, understanding, and using the data.⁵⁸ In fact, Facebook explicitly uses the hashed

⁵⁷ “Udff[–]” parameters are used by Facebook in “advanced matching” and the “letters or numbers in between the brackets are shorthand for the data being sent. For example, [em] means email. Facebook has a table where [one] can look these abbreviations up.” Maria Puertas & Simon Fondrie-Teitler, THE MARKUP, *In 2023, Resolve to Fix your Organization’s Meta Pixel Problem* (Jan. 31, 2023), <https://themarkup.org/levelup/2023/01/31/in-2023-resolve-to-fix-your-organizations-meta-pixel-problem> (last visited Feb. 16, 2023).

⁵⁸ See <https://www.facebook.com/business/help/112061095610075?id=2469097953376494>; <https://www.facebook.com/business/help/611774685654668?id=12053%2076682832142>

information it gathers to link Pixel-transmitted data to Facebook profiles.⁵⁹ Indeed, there would be no value in targeting Facebook users with Defendant's ads if Facebook couldn't read the hashed data it received from Defendant to know who to target.

144. As Facebook explains, "Automatic advanced matching will tell your pixel to look for recognizable form fields and other sources on your website that contain information such as first name, last name and email address. The Meta Pixel receives that information along with the event, or action, that took place. This information gets hashed in the visitor's browser. *We can then use the hashed information to more accurately determine which people took action in response to your ad.*"⁶⁰ Similarly, Facebook tells businesses: "When you upload your customer list in Ads Manager to create a Custom Audience, the information in your list is hashed before it's sent to Facebook. *Facebook uses this hashed information and compares it to our own hashed information. Then, we help build your audience by finding the Facebook profiles that match and create a Custom Audience for you from those matches.*"⁶¹ In other words, Facebook uses its own secret language to encode and then read and match individuals' information.

145. Facebook claims that after hashing individuals' Private Information (including their personal identifiers and PHI shared by Defendant) and matching it to Facebook profiles to create Custom Audiences, Facebook deletes the hashed data. Even assuming this is true, by that point, damage has already occurred—Facebook has read, understood, analyzed, and expressly taken action to match the shared PHI with specific individuals, with the express purpose of targeting

⁵⁹ See <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

⁶⁰ <https://www.facebook.com/business/help/611774685654668?id=12053%2076682832142>

⁶¹ <https://www.facebook.com/business/help/112061095610075?id=2469097953376494>

those individuals with ads based on their data (here, PHI) that was shared and used to create Defendant's Custom Audiences—all at Defendant's request.

146. This disclosed PHI and PII allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting Defendant to target those persons with Defendant's ads, Facebook also then sells that information to marketers who will online target Plaintiffs and Class Members.

147. Through these events, Aspen disclosed to Facebook (i) when Users viewed Aspen's locations and services, (ii) Users' search activities, (iii) treatments and services Users sought, (iv) when Users scheduled appointments and (v) Users' PII including names, email addresses, phone numbers and other unique personal identifiers.

148. The Pixels also share Users' identifying information for easy tracking via the cookies stored on their devices by Facebook, Google, including the `_fbp`, `datr`, `fr`, `_ga_`, and `_gid`. Accordingly, without any User action or authorization, Defendant commands Plaintiffs' and Class Members' computing devices to contemporaneously re-direct the Plaintiffs' and Class Members' unique personal identifiers contained in those cookies as well as the content of their communications, to Facebook and/or Google.

149. Importantly, the Private Information Defendant's Meta Pixel sent to Facebook was sent alongside the Plaintiffs' and Class Members' Facebook ID (`c_user` cookie or FID), thereby allowing individual patients' communications with Defendant and the Private Information contained in those communications to be linked to their unique Facebook accounts.

150. Because Aspen includes the `c_user` cookie in the data sent to Facebook, tools such as VPNs are insufficient to hide a User's identity. VPNs anonymize users' IP addresses, however,

since the `c_user` cookie specifically identifies the User's Facebook profile, Facebook knows exactly who the User is regardless of the User's IP address.

151. In addition, Aspen also sent Users' phone numbers and email addresses to Facebook by enabling the Advance Matching feature for the Pixel, which Facebook can – and does – match to its own database of Facebook users.

152. Aspen also includes browser fingerprints and other identifying information in the data sent to Facebook. Browser fingerprints include details about the User's operating system and monitor screen size which remain consistent across multiple browsers. As mentioned *supra*, browser fingerprinting techniques can successfully identify 99.24 percent of all users.

153. Even more sophisticated Users who use ad blockers could not have prevented their Private Information being sent to Facebook by Aspen's embedded Meta Pixel (or other Pixel data recipients) because ad blockers work by blocking certain domains – which users never visit. If a User blocked the facebook.com domain, then the User would not be able to view Facebook at all – which is a highly unlikely situation (especially for someone with an active Facebook account).

G. Aspen Commoditized Users' Private Information for its Gain.

154. After intercepting and collecting this information, Facebook (and other third parties that gather such information for marketing and analytics) processed, analyzed and assimilated it into datasets like Core Audiences and Custom Audiences.

155. With respect to Facebook, if the website visitor is also a Facebook user, the information collected via the Meta Pixel is associated with the user's Facebook ID ("FID") that identifies their name and Facebook profile, *i.e.*, their real-world identity.

156. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user including pictures, personal interests, work history, relationship status and other details.

157. Because the user's FID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the FID to locate, access and view the user's corresponding Facebook profile quickly and easily.

158. This disclosed Private Information allows third parties like Facebook and other third parties to know that a specific patient is seeking confidential medical care and the type of medical care being sought (in the case of Aspen, dental health care). Third parties then use this information—without patient consent—to target them with advertisements.

159. For example, if a patient searched for a dental health provider to treat emergency dental care, this information would be transmitted to third parties and then used to target Aspen patients with advertisements for third-party drugs and services related to emergency dental care.

160. Aspen was similarly able to use this information to target its patients “more effectively” with Aspen advertisements for its own services.

161. Thus, by utilizing the Pixel, the cost of Aspen advertising and retargeting was reduced, thereby benefiting and enriching Aspen.

162. Aspen's tapping and brokering of this Private Information was highly lucrative for both Aspen and Facebook.

163. Aspen used the Pixel to help, among other things, monitor traffic on its Site, send targeted advertising to Site visitors after they navigated to other sites and increase revenue and profits. In exchange, Facebook was given a “backdoor” into all of Aspen's patients' confidential online communications in the form of a secret web-based wiretap.

164. Aspen's and Facebook's *quid pro quo*, however, was at Plaintiffs' expense because it was their (and the putative class members') highly sensitive Private Information brokered and commoditized for targeted advertising.

H. Plaintiffs and Class Members Did Not Provide Authorization to Defendant or Facebook to Disclose Their PHI To Facebook

165. When an individual creates a Facebook account, they enter into an agreement with Facebook by accepting and acknowledging the Terms of Service, Data Policy/Privacy Policy, and Cookie Policy. This agreement is confirmed through a checkbox on the sign-up page. Both Facebook and its users are obligated to abide by these binding Terms of Service and Policies.

166. Although the Facebook Data Policy makes general broad disclosures about the data it collects, the scope of Facebook's "data license" is not unlimited. For example, by signing up for Meta, a Facebook user has not agreed to exchange with Facebook the right for Facebook to obtain their bank account information or Social Security number.

167. The Facebook Privacy Policy does not state that Facebook actively solicits Facebook users' healthcare providers, health insurers, pharmacies, prescription drug companies, and other covered entities under 45 C.F.R. § 160.103 to become Facebook Partners using Facebook's business services.

168. The Facebook Privacy Policy does not state that, in exchange for use of its Products, Facebook will collect health information from a Facebook user's healthcare providers, health insurers, pharmacies, prescription drug companies, or other covered entities under 45 C.F.R. § 160.103 about the Facebook user, including their communications, actions, and status as patients with those health entities.

169. Facebook Data Policy explicitly states that businesses utilizing the Pixel are

obligated to possess legal rights to collect, use, and share user data before sharing any data with Facebook.⁶²

170. However, Facebook does not verify whether the businesses utilizing the Pixel have indeed obtained the necessary consent. Instead, Facebook relies on its business customers to police themselves. Businesses need only “represent and warrant” that they have adequately and prominently notified users about the collection, sharing, and usage of data through their Business Tools.⁶³

171. Facebook’s contract with healthcare providers for use of the Meta Pixel does not mention HIPAA.

172. Defendant does not have legal authority to use or share Plaintiffs’ and Class Members’ Private Information with Facebook as this information is protected under HIPAA and other federal and state laws.

173. In essence, when Facebook contracts with a healthcare provider like Defendant, both entities fail to ensure compliance with their own Terms of Service and/or privacy policies, as well as state and federal laws protecting sensitive health information.

I. *Aspen Knew that the Meta Pixel Would Reveal Its Users’ Private Information to Facebook – As Intended By Facebook*

174. Due to the nature of how the Meta Pixel functions, Aspen knows or should have known that its Users’ sensitive PHI would be transmitted to Facebook when Users engaged in any

⁶² *Meta Business Help Center: About restricted Meta Business Tools Data*, <https://www.facebook.com/business/help/1057016521436966?id=188852726110565> (last visited on Feb. 14, 2024).

⁶³ Before April 2018, Meta’s contract did not require its business “partners” to have the lawful right to share user data before doing so.

interactions on the Website, including looking up treatments and services and booking appointments.

175. Upon information and belief, Aspen did not contractually limit how Facebook could use the sensitive data it received from the Website.

176. Despite its recent pronouncements, Facebook is also aware that by allowing healthcare providers to implement the Meta Pixel, it facilitates the gathering of PHI from patients of those healthcare providers – and uses this sensitive data to improve its advertising processes.

177. Facebook does not use an advanced technical system to monitor whether Meta Collection Tools are installed on websites that will transmit PHI to Facebook, or to filter out incoming PHI. To the contrary, Meta Health, a division of Meta dedicated to healthcare marketing, urges healthcare providers and other covered entities to use Meta Collection Tools to target ads to patients.

178. Meta Health maintains a page where Facebook offers advertisers the chance to “get help growing your healthcare business” and explains how “Healthcare marketers are partnering with Meta.”⁶⁴

179. Meta Health is dedicated to helping web developers and advertisers in healthcare related industries to increase their marketing spend with Facebook and improve their marketing campaigns using Meta Collection Tools.

180. Meta Health’s role is to “inform” healthcare marketers “to think about how we can really disrupt health and how we market to patients.”⁶⁵ Meta Health employees are assigned to

⁶⁴ See <https://www.facebook.com/business/industries/consumer-goods/healthcare> (last visited Feb. 16, 2024).

⁶⁵ *Facebook Disrupting Health: A Conversation with Jasson Gilmore*,

specific healthcare providers and other covered entities to encourage and aid their use of Meta Collection Tools for targeting patients.

181. Facebook provides guidance and resources for web developers and advertisers for the healthcare industry on a dedicated webpage at <https://www.facebook.com/business/industries/health>. Among other things, this webpage includes examples of advertising campaigns so that web developers and advertisers can “See how health brands are reaching new audiences with Facebook advertising.”

182. Facebook has engaged in advertising campaigns relating to treatments for allergies, arthritis, birth control, diabetes, erectile dysfunction, hair loss, high cholesterol, migraines, and many more prescription drugs and treatments.⁶⁶

183. Facebook is able to run such targeted campaigns precisely due to the sensitive nature of health information it receives from websites like Aspen’s that utilize its Business Tools including the Meta Pixel.⁶⁷

184. To that point, a complaint by the Federal Trade Commission filed in 2020 exhibited that Facebook received medical information through its Business Tools for years. The FTC

<https://www.facebook.com/business/industries/health?deeplink=829704181304626> (last visited Feb. 16, 2024).

⁶⁶ See generally *Get winning advertising solutions from businesses like yours* (2023), <https://www.facebook.com/business/success/categories/health-pharmaceuticals> (last visited Feb. 16, 2024). The “marketing case studies” on this page change on occasion.

⁶⁷ See, e.g., Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report*, NEWSBYTES (June 16, 2022) <https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story> (last visited Feb. 16, 2024).

concluded that Facebook had used that sensitive information for their own research and development purposes.⁶⁸

185. The New York State Department of Financial Services (NYSDFS) reached a similar determination. It found that Facebook had collected sensitive data, including medical information, in violations of its own policies. NYSDFS stated that “[m]erely stating a rule, however, has little meaning if the rule is not enforced, and the unfortunate fact is that Facebook does little to track whether . . . developers are violating this rule and takes no real action against developers that do.”⁶⁹ The NYSDFS stated that “Facebook’s efforts here [are] seriously lacking” and that “[u]ntil there are real ramifications for violating Facebook’s policies, Facebook will not be able to effectively prohibit the sharing of sensitive user data with third-parties.”⁷⁰

186. An article by the Markup also reported that its investigation into Facebook’s “filtering” system revealed that Facebook failed to delete the most obvious forms of sexual health information, which included the URLs with information related to abortion, which stated “postabortion,” “i-think-im-pregnant” and “abortion-pill.”⁷¹

187. A research director at UC Berkeley in the Usable Security and Privacy Group has stated that Facebook just does not have the incentive to enforce its own privacy policies because

⁶⁸ See FTC, *In the Matter of FLO HEALTH, INC.*, Complaint, at *5 (2020), https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf (last visited Feb. 16, 2024).

⁶⁹ *Report on Investigation of Facebook Inc. Data Privacy Concerns*, p. 16 (February 18, 2021) (last visited Feb. 16, 2024).

⁷⁰ *Id.* at p. 17.

⁷¹ Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients* (June 15, 2022), <https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients> (last visited Feb. 16, 2024).

“[t]hat costs them money to do. As long as they’re not legally obligated to do so, why would they expend any resources to fix [it]?”⁷²

188. Additionally, documents leaked to the news organization Vice in 2021 exposed that Facebook’s employees acknowledged or confirmed Facebook’s inability to effectively manage the way its systems utilize data. A Facebook engineer working on the Ad and Business Product team stated that “We do not have adequate level of control and explainability over how our systems use data, and thus we can’t confidently make controlled policy changes or external commitments such as ‘we will not use X data for Y purpose.’”⁷³

189. Despite Facebook’s history of receiving and misusing users’ health data from its business partners, Aspen purposefully disclosed Plaintiffs’ and Class Members’ sensitive health communications, including Private Information, without their consent to Facebook to improve the effectiveness of its advertising and marketing.

J. Google Analytics.

190. Alphabet Inc., the parent holding company of Google, generates revenues primarily by delivering targeted online advertising through Google, which is the creator of the Google Source Code and an established advertising company.

191. Google Source Code—the source code associated with Google’s advertising system and products, including Google Analytics—is designed to track and collect individuals’ information when they are using the Internet.

⁷² See *id.*

⁷³ Lorenzo Franceschi-Bicchierai, *Facebook Doesn’t Know What It Does With Your Data, Or Where It Goes: Leaked Document* (April 26, 2022), <https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes> (last visited Feb. 16, 2024).

192. Google Analytics is associated with the domains www.Google-Analytics.com and analytics.google.com.

193. Google Source Code is provided by Google in a copy-and-paste format, and its functionality is uniform on all web properties, with the option for website operators like Aspen to choose to disclose additional data about its users to Google. Its operation is hidden by Google's design and does not indicate to users that Google Source Code is present on a website they are visiting.

194. When the Google Source Code is placed by website operators such as Aspen on its website, Aspen's actions allow the Google Source Code to instruct the computer accessing Aspen's home page to track, intercept, and redirect the user's information to Google.

195. This tracking, interception, and redirection of information occurs when individuals exchange communications or requests with the relevant websites.

196. Google Analytics, a marketing tool used for advertising and analytics, is one of Google's primary products and services that leverage Google Source Code to track, collect, and subsequently use (*i.e.*, monetize) individuals' personal information. A fundamental and primary purpose of Google Analytics is to obtain information about consumers' communications and activities that is accessible by entities other than Google. Google accomplishes this through Google Analytics, in part, by touting it as a tool that enables clients to "understand the customer journey and improve marketing ROI."⁷⁴

197. Specifically, according to Google, Google Analytics is intended to help advertisers:

⁷⁴ Google Marketing Platform, Analytics, <https://marketingplatform.google.com/about/analytics/> (last visited Feb. 13, 2024).

- a. “Unlock customer-centric measurement” to “[u]nderstand how your customers interact across your sites and apps, throughout their entire lifecycle;”
- b. “Get smarter insights to improve ROI,” to “[u]ncover new insights and anticipate future customer actions with Google’s machine learning to get more value out of your data” and
- c. “Connect your insights to results,” to “[t]ake action to optimize marketing performance with integrations across Google’s advertising and publisher tools[.]”⁷⁵

198. Like the Meta Pixel, when a user exchanges information with the host of a website—such as through a search query—Google Source Code operates to surreptitiously direct the user’s browser to send a separate message to Google’s servers. This second, secret transmission contains the original request sent to the host website, (“GET request”), along with additional data that the Google Source Code is configured to collect (“POST request”). These transmissions are initiated by Google Source Code and concurrent with the communications to and from the host website.

199. Google Analytics offers website developers like Aspen the option to include additional data of their own choosing about its users’ activities in any communications to Google, including “Event Value” and “Event Label” data. As can be seen from the Google Analytics developer website, this data is optional and not sent to Google by default:⁷⁶

⁷⁵ *Id.*

⁷⁶ Google Analytics, Measurement Protocol Parameter Reference, <https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters> (last visited Feb. 13, 2024).

Google Analytics > Measurement > Measurement Protocol (Universal Analytics)

Event Action

Required for event hit type.

Specifies the event action. Must not be empty.

Parameter	Value Type	Default Value	Max Length	Supported Hit Types
ea	text	None	500 Bytes	event

Example value: Action
Example usage: ea=Action

Event Label

Optional.
Specifies the event label.

Parameter	Value Type	Default Value	Max Length	Supported Hit Types
e1	text	None	500 Bytes	event

Example value: Label1
Example usage: e1=Label1

Event Value

Optional.
Specifies the event value. Values must be non-negative.

Parameter	Value Type	Default Value	Max Length	Supported Hit Types
ev	integer	None	None	event

Example value: 55
Example usage: ev=55

Hit type
Non-Interaction Hit
Content Information
Document location URL
Document Host Name
Document Path
Document Title
Screen Name
Content Group
Link ID
Apps
Application Name
Application ID
Application Version
Application Installer ID
Events
Event Category
Event Action
Event Label
Event Value
E-Commerce
Transaction ID
Transaction Affiliation
Transaction Revenue
Transaction Shipping
Transaction Tax
Item Name
Item Price
Item Quantity
Item Code
Item Category
Enhanced E-Commerce
Product SKU
Product Name
Product Brand
Product Category
Product Variant

200. In addition, upon information and belief, Aspen chose to disclose search terms users entered into the Aspen Site and information disclosed in the patient portal, to Google via Google Analytics by enabling the Google Analytics “Enhanced event measurement” feature.

[GA4] Enhanced event measurement

Discover how to enable and disable enhanced event measurement and learn more about which parameters are collected for each event.


Enhanced measurement lets you measure interactions with your content by enabling options (events) in the Google Analytics interface. No code changes are required. When you enable these options for a web data stream, your Google Analytics tag starts sending events right away.

Before turning on the enhanced measurement feature, be sure you understand each option and what enhanced data will be collected. You can also turn off specific measurement options in settings.



You're required to ensure that no [personally identifiable information](#) is collected.

Enable or disable enhanced event measurement

1. In [Google Analytics](#), click [Admin](#).
2. [Make sure you are in the correct account and property.](#)
3. In the *Property* column, click **Data Streams > Web**.
4. Under *Enhanced measurement*, slide the switch **On** to enable all options. Click  to edit individual options as needed.



201. In other words, Aspen took affirmative, additional steps of its own to configure Google Analytics' tracking's ability to ensure that Google received additional data about its website users.

202. Also like the Meta Pixel, Google associates the information it obtains via Google Source Code with other information regarding the user, using personal identifiers that are transmitted concurrently with other information the code is configured to collect.

203. These identifiers include the "cid," a combination of the time at which the user visited the website and a unique identifier. The "cid" is assigned to an individual's browser and can persist for up to two years, allowing Google to link a series of events to the same browser and, thus, to an individual. For Google account holders, this identifier is also linked to that account.

204. In addition to information gleaned from a user's "cid," Google can create a unique, digital "fingerprint" for a user based on data transmitted via Google Source Code, which allows Google to link certain web activity to a user. This "fingerprint" can consist of information regarding a user's screen depth, screen resolution, browser name and version, and operating system name and version, as well as a user's Internet Protocol ("IP") address. With that information, Google is able to link data acquired through Google Analytics to a particular user.

205. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.⁷⁷

206. Browser-fingerprints are also considered personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors. Browser-fingerprints are protected personal identifiers under HIPAA.

207. After tracking, intercepting and acquiring user's information, Google uses the information for personalized advertising in its advertising systems which includes, but is not limited to, Google Analytics.⁷⁸

208. For example, Google Analytics uses the information it collects to facilitate its Audience Targeting feature. Audience Targeting refers to serving ads to only a select number of users who share certain common characteristics. For Google's Audience Targeting, Google can target ads to either "Pre-defined Google Audiences" or "Advertiser-curated Audiences." Pre-defined Audiences are those created by Google based on interest and demographic data.

⁷⁷ See Yinzhi Cao, Song Li, Erik Wijmans, *(Cross-)Browser Fingerprinting via OS and Hardware Level Features* (February 27, 2017), <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/> (last visited Feb. 13, 2024).

⁷⁸ See 45 C.F.R. § 164.514(b)(2)(i)(M), (R).

209. Advertiser-curated Audiences are customized audiences created by Google through the use of the Source Code, including audiences created through Google Analytics. Like Meta, Google is therefore able to monetize the information surreptitiously intercepted, with Aspen's help, from visitors to the Aspen Site.

K. The Use of Tracking Technologies on Public-Facing Pages Violates the Law.

210. The fact that Aspen used tracking technologies on public-facing pages of its Website is *not* dispositive of its liability because Users' Private Information was shared from Aspen's public-facing Site including, for example, the User's phone number and email address which they provided to Aspen in the process of making an appointment, along with the details of the appointment.

211. OCR is clear that the prohibition against tracking technologies disclosing PHI applies to public-facing websites, which are not protected by passwords (*i.e.*, those that do not require account creation or other authenticated access):

[T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, *dedicated* login page), or a user registration webpage where an individual creates a login for the patient portal ... ***[and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permit[] individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances.*** For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor,

and thus the HIPAA Rules apply.⁷⁹

212. The Bulletin also makes clear that the user of a website does ***not*** have to be an existing patient of the regulated entity for HIPAA Rules to apply:

Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. *All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e. it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.*⁸⁰

213. Here, Aspen placed the Pixel on its public-facing webpages including those where an individual could schedule an appointment. And, to confirm the appointment, a patient had to provide the type of appointment they wanted (emergency, broken tooth/tooth pain, dental implants,

⁷⁹ OCR Bulletin, *supra*, note 19 (emphasis added); *see also Cousin v. Sharp Healthcare*, 2023 WL 8007350, at *2 (S.D. Cal. Nov. 17, 2023) (J. Anello denied motion to dismiss plaintiffs' privacy claims alleging healthcare provider collected and shared their browsing activity related to provision of healthcare, to the extent defendant sought to dismiss all of plaintiffs' claims because a public-facing website was at issue); *In re Meta Healthcare Pixel Litigation*, 2024 WL 333883, at *1-7 (N.D. Cal. Jan. 29, 2024) (J. Orrick denying motion to dismiss and finding that plaintiffs' privacy claims were not foreclosed simply because their communications with their healthcare providers may have been through publicly available webpages).

⁸⁰ *Id.*

dentures, aligners or other/checkup) along with their name, date of birth, location for the appointment, email address and phone number.

214. As a result, even on the public-facing Site, Aspen tracked Users' specific medical requests, the fact that they were making an appointment and the fact that they did make appointments at specific locations.

215. Aspen collected this Private Information in order to combine it with individuals' unique personal identifiers including, but not limited to, their phone number, email address and IP address—all of which was then shared with Facebook with the patient's unique FID.

216. It is clear that Aspen's collection and divulgence of Private Information without consent on webpages that do not require Users to log in ("unauthenticated" webpages) and even where the User does not have an established relationship with the medical provider is illegal.

L. Aspen's Use of Tracking Technologies Such as the Pixels Violates HIPAA.

217. Under federal law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient or household member of a patient for marketing purposes without the patients' express written authorization.

218. Guidance from HHS instructs healthcare providers that patient status alone is protected by HIPAA.

219. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;"

and either (i) “identifies the individual;” or (ii) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

220. The Privacy Rule broadly defines protected health information as individually identifiable health information that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103. Under the HIPAA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination” or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

- A. Names;
- ...
- H. Medical record numbers;
- ...
- J. Account numbers;
- ...
- M. Device identifiers and serial numbers;
- N. Web Universal Resource Locators (URLs);
- O. Internet Protocol (IP) address numbers; ... and
- P. Any other unique identifying number, characteristic, or code... and the covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”⁸¹

⁸¹ 45 C.F.R. § 160.514 (cleaned up).

221. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI.

222. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, “[i]f such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.”⁸²

223. Consistent with this restriction, HHS has issued marketing guidance that provides, “With limited exceptions, the [Privacy] Rule requires an individual’s written authorization before a use or disclosure of his or her protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.”⁸³

224. Here, as described *supra*, Aspen provided patient information to third parties in violation of the Privacy Rule – and its own Privacy Policy.

⁸² See *HHS Guidance Regarding Methods for De-identification of PHI*, *supra*, note 18.

⁸³ *Marketing*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html> (last visited Feb. 13, 2024).

225. HIPAA also requires Aspen to “review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(c), and to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights,” 45 C.F.R. § 164.312(a)(1) – which Aspen failed to do.

226. Aspen further failed to comply with other HIPAA safeguard regulations as follows:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that Aspen created, received, maintained, and transmitted in violation of 45 C.F.R. section 164.306(a)(1);
- b. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);
- c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Aspen in violation of 45 C.F.R. section 164.308(a)(6)(ii);
- d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);
- e. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3) and
- f. Failing to design, implement, and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

227. Commenting on a June 2022 report discussing the use of Meta Pixel by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, “I am deeply troubled by what [the hospitals]

are doing with the capture of their data and the sharing of it ... It is quite likely a HIPAA violation.”⁸⁴

228. Aspen’s placing a third-party tracking code on its Website is a violation of Plaintiffs’ and Class Members’ privacy rights under federal law. While Plaintiff does not bring a claim under HIPAA itself, this violation demonstrates Aspen’s wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

M. Aspen’s Use of Tracking Technologies Including the Pixels Violates OCR Guidance.

229. In addition, the federal government has issued guidance warning that tracking technologies like the Pixels may come up against federal privacy law when installed on healthcare websites.

230. As mentioned previously, healthcare organizations regulated under the HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixels *only in a limited way*, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients’ PHI to these vendors.⁸⁵

231. According to the Bulletin, Aspen has violated HIPAA rules by implementing the Pixels.⁸⁶

⁸⁴ ‘Deeply Troubled’: Security experts worry about Facebook trackers on hospital sites, ADVISORY BOARD, <https://www.advisory.com/daily-briefing/2022/06/17/data-trackers> (last visited Feb. 13, 2024).

⁸⁵ See OCR Bulletin, *supra*, note 19.

⁸⁶ See *id.* (“disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures”).

232. Aspen has shared Plaintiffs' and Class Members' Private Information including health conditions for which they seek treatments; treatments and/or medications sought; the frequency with which they take steps to obtain healthcare for certain conditions; and their unique personal identifiers. This information is, as described in the OCR Bulletin, "highly sensitive."

233. The OCR Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, *or any unique identifying code*.⁸⁷

234. Aspen's sharing of Private Information to third parties including Facebook and/or Google violated Plaintiffs' and Class Members' rights to privacy and confidentiality in their receipt of healthcare services and fell below the applicable standard for safeguarding the confidential Private Information of Plaintiffs and Class Members.

N. Aspen Violated Industry Standards.

235. It is a cardinal rule that a medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship.

236. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

237. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)[.]

⁸⁷ *Id.* (emphasis added).

238. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

239. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically...must: (c) Release patient information only in keeping ethics guidelines for confidentiality.⁸⁸

240. Defendant's use of the Pixels also violates FTC data security guidelines. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

241. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*⁸⁹ established cyber-security guidelines for businesses.

⁸⁸ AMA Principles of Medical Ethics: I, IV, *Chapter 3: Opinions on Privacy, Confidentiality & Medical Records*, <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf>, [American Medical Association](https://www.ama-assn.org) (last visited Feb. 13, 2024).

⁸⁹ *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 13, 2024).

242. These guidelines state that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network vulnerabilities; and implement policies to correct any security problems.

243. Defendant failed to implement these basic, industry-wide data security practices.

O. Users' Reasonable Expectation of Privacy.

244. Plaintiffs and Class members had a reasonable expectation of privacy and confidentiality when they sought medical services from Defendant via its Site.

245. Indeed, at all times when Plaintiffs and Class Members provided their PII and PHI to Defendant, they each had a reasonable expectation that the information would remain confidential and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

246. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

247. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.⁹⁰

⁹⁰ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/> (last visited Feb. 13, 2024).

248. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class members.

P. Unique Personal Identifiers are Protected Health Information.

249. While not all health data is covered under HIPAA, the law specifically applies to healthcare providers, health insurance providers and healthcare data clearinghouses.⁹¹

250. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

251. These HIPAA Identifiers, as relevant here, include names, dates related to an individual, email addresses, device identifiers, web URLs and IP addresses.⁹²

252. Aspen improperly disclosed Plaintiffs' and Class Members' HIPAA identifiers, including their names, emails, dates they sought treatments, computer IP addresses, device identifiers, and web URLs visited to Facebook, Google and likely other third parties through their use of the Pixels *in addition to* services selected, patient statuses, medical conditions, treatments, provider information and appointment information.

⁹¹ See Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook* (June 21, 2022), <https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook> (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations") (last visited Feb. 13, 2024).

⁹² See HHS Guidance Regarding Methods for De-identification of PHI, *supra*, note 18.

253. An IP address is a number that identifies the address of a device connected to the Internet. IP addresses are used to identify and route communications on the Internet. IP addresses of individual Internet users are used by Internet service providers, websites and third-party tracking companies to facilitate and track Internet communications.

254. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

255. Facebook, Google and other third-party marketing companies track IP addresses for targeting individual homes and their occupants with advertising.

256. Under HIPAA, an IP address is considered personally identifiable information, which is defined as including “any unique identifying number, characteristic or code” and specifically listing IP addresses among examples.⁹³

257. HIPAA further declares information as personally identifiable where the covered entity has “actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

258. Consequently, Aspen’s disclosure of Plaintiffs’ and Class Members’ IP addresses violated HIPAA and industry-wide privacy standards.

⁹³ *See* 45 C.F.R. § 164.514 (2).

Q. Aspen Was Enriched & Benefitted from the Use of the Pixel & other Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein.

259. One of the primary reasons that Aspen decided to embed Pixels and other tracking technologies on its Website was to improve marketing by creating campaigns that maximize conversions and thereby decrease costs to Aspen and boost its revenues.

260. Meta advertises its' Pixel as a piece of code "that can help you better understand the *effectiveness of your advertising* and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system *decrease your costs*."⁹⁴

261. Retargeting is a form of online marketing that targets Users with ads based on previous internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.⁹⁵

262. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Aspen's website. For example, if a new member signs up to use Aspen, then that information is sent to Facebook. Facebook can then use

⁹⁴ *What is the Meta Pixel*, <https://www.facebook.com/business/tools/meta-pixel> (emphasis added) (last visited Feb. 13, 2024).

⁹⁵ *The complex world of healthcare retargeting*, <https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/> (last visited Feb. 13, 2024).

its data on the User to find more users to click on a Aspen ad and ensure that those users targeted are more likely to convert.⁹⁶

263. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, “includes URL names of pages visited, and actions taken - all of which could be potential examples of health information. If the Meta Pixel can see that a visitor navigated to a page on diabetes treatment, is that considered health information? Yes, it certainly is.”⁹⁷

264. Plaintiffs’ and Class Members’ Private Information has considerable value as highly monetizable data especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

265. In exchange for disclosing the Private Information of their accountholders and patients, Aspen is compensated by Facebook, Google and likely other third parties in the form of enhanced advertising services and more cost-efficient marketing on their platform.

266. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many are not HIPAA-complaint or are only HIPAA-compliant if certain steps are taken.⁹⁸

⁹⁶ *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (March 14, 2023), <https://freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking#:~:text=Meta%20isn't%20HIPAA-compliant,a%20personal%20user%20data%20vacuum> (last visited Feb. 13, 2024).

⁹⁷ *Id.*

⁹⁸ See PIWIK Pro, *The guide to HIPAA compliance in analytics*, <https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf> (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Feb. 13, 2024).

267. For example, Freshpaint a healthcare marketing vendor, cautioned that “Meta isn’t HIPAA-compliant”, and “If you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now.”⁹⁹

268. Medico Digital also warns that “retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences.”¹⁰⁰

269. Whether a User has a Facebook profile is not indicative of damages because Facebook creates shadow profiles and at least one court has recognized that the pixels’ ability to track comprehensive browsing history is also relevant. *See, e.g., Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from Websites and Google Cookies that it collects across the internet on the same user).

270. Aspen retargeted patients and potential patients to get more people to purchase their services. These patients include Plaintiffs and Class Members.

271. Thus, utilizing the Pixels directly benefits Aspen by, among other things, reducing the cost of advertising and retargeting.

R. Plaintiffs’ Private Information Has Substantial Value.

272. Plaintiffs’ and Class Members’ Private Information had value, and Aspen’s disclosure and interception harmed Plaintiffs and the Class by not compensating them for the value of their Private Information and in turn decreasing the value of their Private Information.

⁹⁹ *Id.*

¹⁰⁰ *The complex world of healthcare retargeting, supra*, note 95.

273. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

274. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

275. The robust market for Internet user data has been analogized to the “oil” of the tech industry.¹⁰¹ A 2015 article from TechCrunch accurately noted that “Data has become a strategic asset that allows companies to acquire or maintain a competitive edge.”¹⁰² That article noted that the value of a single Internet user—or really, a single user’s data—varied from about \$15 to more than \$40.

276. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200 billion industry wide.

277. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: “Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.”¹⁰³

¹⁰¹ See *The world’s most valuable resource is no longer oil, but data*, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (last visited Feb. 13, 2024).

¹⁰² See <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/> (last visited Feb. 13, 2024).

¹⁰³ Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV.L.REV. 2055, 2056-57

278. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.¹⁰⁴

279. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

280. Courts recognize the value of personal information and the harm when it is disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

281. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

(2004).

¹⁰⁴ *See 10 Apps for Selling Your Data for Cash*, <https://wallethacks.com/apps-for-selling-your-data/> (last visited Feb. 13, 2024).

282. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

283. The value of health data is well-known and various reports have been conducted to identify the value of health data.

284. Specifically, in 2023, the Value Examiner published a report that focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of “such data should ensure it is priced at fair market value to mitigate any regulatory risk.”¹⁰⁵

285. In 2021, Trustwave Global Security published a report entitled *Hackers, breaches and the value of healthcare data*. With respect to healthcare data records, the report found that they may be valued at up to \$250 per record on the black market, compared to \$5.40 for the next highest value record (a payment card).¹⁰⁶

286. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled “*How Your Medical Data Fuels a*

¹⁰⁵ See *Valuing Healthcare Data*, <https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf> (last visited Feb. 13, 2024).

¹⁰⁶ See <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (citing *The Value of Data*, https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf) (last visited Feb. 13, 2024).

Hidden Multi-Billion Dollar Industry,” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.¹⁰⁷

287. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”¹⁰⁸

288. The dramatic difference in the price of healthcare data when compared to other forms of private information that is commonly sold is evidence of the value of PHI.

289. But these rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users’ stolen data, surely Internet users can sell their own data.

290. In short, there is a quantifiable economic value to Internet users’ data that is greater than zero. The exact number will be a matter for experts to determine.

291. Aspen gave away Plaintiffs’ and Class Members’ communications and transactions on its Site without permission.

292. The unauthorized access to Plaintiffs’ and Class Members’ personal and Private Information has diminished the value of that information, resulting in harm to Site Users, including Plaintiffs and Class Members.

293. Plaintiffs have a continuing interest in ensuring that their future communications with Aspen is protected and safeguarded from future unauthorized disclosure.

¹⁰⁷ See <https://time.com/4588104/medical-data-industry/> (last visited Feb. 13, 2024).

¹⁰⁸ See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited Feb. 13, 2024).

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff A.D.

294. Beginning in or around 2023, Plaintiff A.D. started to utilize Aspen's Site to research conditions, treatments, and dental healthcare providers, and schedule appointments. Specifically, Plaintiff A.D. used the Site to make an appointment for a consultation to get dentures and implants for the bottom part of their mouth. Plaintiff A.D. ultimately had surgical extractions and received dentures and implants in May 2023.

295. While seeking those services and treatments, Aspen required Plaintiff to provide—and Plaintiff provided— Private Information including their first and last name, birth date, email address, phone number and reason for visit.

296. While searching Aspen's specific services, the Website presented numerous guided questions, and then asked Plaintiff to respond, including asking Plaintiff to provide information regarding the reason for their visit.

297. While Plaintiff A.D. was a user of Aspen's services, they never consented to or authorized the use of their Private Information by third parties or to Aspen enabling third parties to access, interpret and use such Private Information.

298. Plaintiff A.D. had an active Facebook account while they used Aspen's services and they accessed Aspen's Website while logged into their Facebook account on the same device.

299. Plaintiff A.D. does not post about their medical conditions on social media.

300. After providing Private Information to Aspen through the Website, Plaintiff A.D. immediately began seeing targeted health ads as they scrolled through their Facebook account,

including ads for dental treatments, including dentures and implants, and for dental healthcare providers in their area.

Plaintiff C.A.

301. Beginning in or around March 2022, Plaintiff C.A. started to utilize Aspen's Website to create an account, research conditions, treatments, and dental healthcare providers, and schedule appointments. Specifically, Plaintiff C.A. scheduled a routine checkup.

302. While seeking those services and treatments, Aspen required Plaintiff to provide—and Plaintiff provided— Private Information including their first and last name, birth date, email address, phone number and reason for visit.

303. While searching Aspen's specific services, the Website presented numerous guided questions, and then asked Plaintiff to respond, including asking Plaintiff to provide information regarding the reason for their visit.

304. While Plaintiff C.A. was a user of Aspen's services, they never consented to or authorized the use of their Private Information by third parties or to Aspen enabling third parties to access, interpret and use such Private Information.

305. Plaintiff C.A. had an active Facebook account while they used Aspen's services and they accessed Aspen's Website while logged into their Facebook account on the same device.

306. Plaintiff C.A. does not post about their medical conditions on social media.

Plaintiff R.G.

307. Beginning in or around the middle of 2022, Plaintiff R.G. started to utilize Aspen's Site to research conditions, treatments, and dental healthcare providers, and schedule appointments.

308. While seeking those services and treatments, Aspen required Plaintiff to provide—and Plaintiff provided—Private Information including their first and last name, birth date, email address, phone number and reason for visit.

309. While searching Aspen's specific services, the Website presented numerous guided questions, and then asked Plaintiff to respond, including asking Plaintiff to provide information regarding the reason for their visit.

310. While Plaintiff R.G. was a user of Aspen's services, they never consented to or authorized the use of their Private Information by third parties or to Aspen enabling third parties to access, interpret and use such Private Information.

311. Plaintiff R.G. had an active Facebook account while they used Aspen's services and they accessed Aspen's Website while logged into their Facebook account on the same device.

312. Plaintiff R.G. does not post about their medical conditions on social media.

313. After providing Private Information to Aspen through the Website, Plaintiff R.G. immediately began seeing targeted health ads as they scrolled through their Facebook account, including ads for dental treatments and for dental healthcare providers in their area.

Plaintiff T.B.

314. Beginning in or around January 2023, Plaintiff T.B. started to utilize Aspen's Site to research conditions, treatments, and dental healthcare providers, and schedule an appointment for general cleaning and cavity filling.

315. While seeking those services and treatments, Aspen required Plaintiff to provide—and Plaintiff provided— Private Information including their first and last name, birth date, email address, phone number and reason for visit.

316. While searching Aspen's specific services, the Website presented numerous guided questions, and then asked Plaintiff to respond, including asking Plaintiff to provide information regarding the reason for their visit.

317. While Plaintiff T.B. was a user of Aspen's services, they never consented to or authorized the use of their Private Information by third parties or to Aspen enabling third parties to access, interpret and use such Private Information.

318. Plaintiff T.B. had an active Facebook account while they used Aspen's services and they accessed Aspen's Website while logged into their Facebook account on the same device.

319. Plaintiff T.B. does not post about their medical conditions on social media.

320. After providing Private Information to Aspen through the Website, Plaintiff T.B. immediately began seeing targeted health ads as they scrolled through their Facebook account, including ads for dental grants.

Plaintiff E.W.

321. Beginning in or around October 2022, Plaintiff E.W. started to utilize Aspen's Site to research conditions, treatments, and dental healthcare providers, and schedule appointments. Plaintiff E.W. ultimately scheduled multiple routine checkups on the Site.

322. While seeking those services and treatments, Aspen required Plaintiff to provide—and Plaintiff provided— Private Information including their first and last name, birth date, email address, phone number and reason for visit.

323. While searching Aspen's specific services, the Website presented numerous guided questions, and then asked Plaintiff to respond, including asking Plaintiff to provide information regarding the reason for their visit.

324. While Plaintiff E.W. was a user of Aspen's services, they never consented to or authorized the use of their Private Information by third parties or to Aspen enabling third parties to access, interpret and use such Private Information.

325. Plaintiff E.W. had an active Facebook account while they used Aspen's services and they accessed Aspen's Website while logged into their Facebook account on the same device.

326. Plaintiff E.W. does not post about their medical conditions on social media.

327. After providing Private Information to Aspen through the Website, Plaintiff E.W. immediately began seeing targeted health ads as they scrolled through their Facebook account, including ads for dental treatments, including dental implants and teeth whitening.

Plaintiff M.H.

328. Beginning in or around May 2023, Plaintiff M.H. started to utilize Aspen's Site to research conditions, treatments, and dental healthcare providers, and schedule an appointment for implant and denture services.

329. While seeking those services and treatments, Aspen required Plaintiff to provide—and Plaintiff provided— Private Information including their first and last name, birth date, email address, phone number and reason for visit.

330. While searching Aspen's specific services, the Website presented numerous guided questions, and then asked Plaintiff to respond, including asking Plaintiff to provide information regarding the reason for their visit.

331. While Plaintiff M.H. was a user of Aspen's services, they never consented to or authorized the use of their Private Information by third parties or to Aspen enabling third parties to access, interpret and use such Private Information.

332. Plaintiff M.H. had an active Facebook account while they used Aspen's services and they accessed Aspen's Website while logged into their Facebook account on the same device.

333. Plaintiff M.H. does not post about their medical conditions on social media.

334. After providing Private Information to Aspen through the Website, Plaintiff M.H. immediately began seeing targeted health ads as they scrolled through their Facebook account, including ads for dental treatments, including implants, veneers, denture replacements, and teeth whitening.

Plaintiff S.B.

335. Beginning in or around 2022, Plaintiff S.B. started to utilize Aspen's Site to research conditions, treatments, and dental healthcare providers, and schedule an appointment for implant services.

336. While seeking those services and treatments, Aspen required Plaintiff to provide—and Plaintiff provided— Private Information including their first and last name, birth date, email address, phone number and reason for visit.

337. While searching Aspen's specific services, the Website presented numerous guided questions, and then asked Plaintiff to respond, including asking Plaintiff to provide information regarding the reason for their visit.

338. While Plaintiff S.B. was a user of Aspen's services, they never consented to or authorized the use of their Private Information by third parties or to Aspen enabling third parties to access, interpret and use such Private Information.

339. Plaintiff S.B. had an active Facebook account while they used Aspen's services and they accessed Aspen's Website while logged into their Facebook account on the same device.

340. Plaintiff S.B. does not post about their medical conditions on social media.

341. After providing Private Information to Aspen through the Website, Plaintiff S.B. immediately began seeing targeted health ads as they scrolled through their Facebook account, including ads for dental treatments and for dental healthcare providers in their area.

TOLLING

342. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know—and had no way of knowing—that their Private Information was intercepted and unlawfully disclosed to Facebook, Google and other third parties because Defendant kept this information secret.

CLASS ALLEGATIONS

343. This action is brought by the representative Plaintiffs on their behalf and on behalf of various classes of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3) and 23(c)(4).

344. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All persons residing in the United States who used Defendant's Website and had Private Information shared with unauthorized third parties including, but not limited to, Facebook during the applicable statutory period.

345. The Illinois Subclass that Plaintiffs A.D., C.A., and R.G. seek to represent is defined as follows:

All persons residing in Illinois who used Defendant's Website and had Private Information shared with unauthorized third parties including, but not limited to, Facebook during the applicable statutory period.

346. The Washington Subclass that Plaintiff E.W. seeks to represent is defined as follows:

All persons residing in Washington who used Defendant's Website and had Private Information shared with unauthorized third parties including, but not limited to, Facebook during the applicable statutory period.

347. The Massachusetts Subclass that Plaintiff S.B. seeks to represent is defined as follows:

All persons residing in Massachusetts who used Defendant's Website and had Private Information shared with unauthorized third parties including, but not limited to, Facebook during the applicable statutory period.

348. The Florida Subclass that Plaintiff M.H. seeks to represent is defined as follows:

All persons residing in Florida who used Defendant's Website and had Private Information shared with unauthorized third parties including, but not limited to, Facebook during the applicable statutory period.

349. Excluded from the proposed Class are any claims for personal injury, wrongful death, or other property damage sustained by the Class; and any Judge conducting any proceeding in this action and members of their immediate families.

350. Plaintiffs reserve the right to amend the definitions of the Class or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

351. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. There are at least 1 million patients that have been impacted by Defendant's

actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendant.

352. **Commonality.** Common questions of law or fact arising from Defendant's conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class members. These common questions include, but are not limited to, the following:

- a) Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class members;
- b) Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class members to Facebook and other unauthorized third parties;
- c) Whether Defendant violated their own privacy policy by disclosing the Private Information of Plaintiffs and Class members to Facebook and other unauthorized third parties;
- d) Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class members that their Private Information would be disclosed to third parties;
- e) Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class members that their Private Information was being disclosed without their consent;
- f) Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized disclosure of patients' Private Information;
- g) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to keep the Private Information belonging to Plaintiffs and Class members free from unauthorized disclosure;
- h) Whether Defendant violated the statutes asserted as claims in this Complaint;
- i) Whether Plaintiffs and Class members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- j) Whether Defendant knowingly made false representations as to their data security and/or privacy policy practices;

- k) Whether Defendant knowingly omitted material representations with respect to their data security and/or privacy policy practices; and
- l) Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their Private Information.

353. **Typicality.** Plaintiffs' claims are typical of those of other Class members because Plaintiffs Private Information, like that of every other Class Member, was compromised as a result of Defendant's incorporation and use of the Pixels and/or other tracking technologies.

354. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

355. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class members in that all the Plaintiffs' and Class members' data was unlawfully stored and disclosed to unauthorized third parties, including Facebook, in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

356. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class

members would likely find that the cost of litigating their individual claim is prohibitively high and would, therefore, have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

357. Defendant has acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

358. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a) Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information and not disclosing it to unauthorized third parties;
- b) Whether Defendant breached a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d) Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;
- e) Whether Defendant breached the implied contract;

- f) Whether Defendant adequately and accurately informed Plaintiffs and Class members that their Private Information would be disclosed to third parties;
- g) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;
- h) Whether Class members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendant's wrongful conduct.

**ILLINOIS LAW SHOULD APPLY TO PLAINTIFFS' &
CLASS MEMBERS' COMMON LAW CLAIMS**

359. The State of Illinois has a significant interest in regulating the conduct of businesses operating within its borders.

360. The State of Illinois has a significant interest in regulating the conduct of businesses operating within its borders.

361. Illinois, which seeks to protect the rights and interests of Illinois and all residents and citizens of the United States against a company headquartered and doing business in Illinois, has a greater interest in the claims of Plaintiffs and the Classes than any other state and is most intimately concerned with the claims and outcome of this litigation.

362. The principal place of business and headquarters of Aspen, located in Illinois, is the "nerve center" of its business activities—the place where its high-level officers direct, control and coordinate its activities, including major policy, financial and legal decisions.

363. Upon information and good faith belief, Defendant's actions and corporate decisions surrounding the allegations made in the Complaint were made from and in Illinois.

364. Defendant's breaches of duty to Plaintiffs and Class Members emanated from Illinois.

365. Application of Illinois law to the Classes with respect to Plaintiffs’ and the Classes’ common law claims is neither arbitrary nor fundamentally unfair because, further to choice of law principles applicable to this action, the common law of Illinois applies to the nationwide common law claims of all Class members. Additionally, given Illinois’ significant interest in regulating the conduct of businesses operating within its borders, and that Illinois has the most significant relationship to Defendant, as it is headquartered in Illinois, there is no conflict in applying Illinois law to non-resident consumers such as Plaintiffs and Class Members. Alternatively, and/or in addition to Illinois law, the laws set forth below apply to the conduct described herein.

CAUSES OF ACTION

COUNT I

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT

18 U.S.C. § 2511(1), *et seq.*

(On behalf of Plaintiffs & the Nationwide Class)

366. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

367. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

368. The ECPA protects both sent and received communications.

369. The ECPA, specifically 18 U.S.C. § 2520(a), provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

370. The transmission of Plaintiffs’ and Class members’ Private Information to Defendant via Defendant’s Website is a “communication” under the ECPA’s definition under 18 U.S.C. § 2510(12).

371. Electronic Communications. The transmission of PII and PHI between Plaintiffs and Class members and Defendant via their Website are “transfer[s] of signs, signals, writing, ... data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

372. Content. The ECPA defines “content” when used with respect to electronic communications to “include[] ***any information concerning the substance, purport, or meaning of that communication.***” 18 U.S.C. § 2510(8) (emphasis added).

373. Interception. The ECPA defines “interception” as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents ... include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

374. Electronical, Mechanical, or Other Device. The ECPA defines “electronic, or other device” as “any device ... which can be used to intercept a[n] ... electronic communication[.]” 18 U.S.C. § 2510(5).

375. The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. The cookies Defendant and Facebook and/or Google use to track Plaintiffs’ and Class Members’ communications;
- b. Plaintiffs’ and Class members’ browsers;
- c. Plaintiffs’ and Class members’ computing devices;
- d. Defendant’s web-servers and
- e. The Pixels deployed by Defendant to effectuate the sending and acquisition of user and patient sensitive communications.

376. Plaintiffs’ and Class Members’ interactions with Defendant’s Website are electronic communications under the ECPA.

377. By utilizing and embedding the Pixels on its Website and/or servers, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class members, in violation of 18 U.S.C. § 2511(1)(a).

378. Specifically, Defendant intercepted Plaintiffs' and Class members' electronic communications via the Pixels, Conversions API and other tracking technologies, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class members' Private Information to third parties such as Facebook and/or Google.

379. Defendant intercepted communications that included, but are not limited to, communications to/from Plaintiffs and Class members containing PII and PHI, including their name, IP address, Facebook ID, appointment scheduling details and health information relevant to the treatments which Plaintiffs and Class members sought from Defendant.

380. This information was, in turn, used by third parties, such as Facebook and/or Google, to 1) place Plaintiffs and Class Members in specific health-related categories and 2) target Plaintiffs and Class Members with particular advertising associated with their specific health conditions. Defendant knowingly transmits this data and does so for the purpose of financial gain.

381. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class members to Facebook, Google and, likely, other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

382. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class members, while knowing or having reason to know that

the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

383. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiffs' and Class members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

384. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information (IIHI) to a third party. HIPAA defines IIHI as:

any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual,* and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.¹⁰⁹

385. Plaintiffs' and Class Members' information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant

¹⁰⁹ 18 U.S.C. § 1320d-(6) (emphasis added).

specifically used the Pixels and other tracking codes to track and utilize Plaintiffs' and Class members' Private Information for its own financial benefit.

386. Defendant was not acting under color of law to intercept Plaintiffs' and Class members' wire or electronic communications.

387. Plaintiffs and Class members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class members' privacy via the Pixels. Plaintiffs and Class members had a reasonable expectation that Defendant would not re-direct their communications content to Facebook, Google or others attached to their personal identifiers in the absence of their knowledge or consent.

388. Any purported consent that Defendant received from Plaintiffs and Class members was not valid.

389. In sending and in acquiring the content of Plaintiffs' and Class members' communications relating to the browsing of Defendant's Website, researching of medical dental conditions and treatments and scheduling appointments with dentists, Defendant's purpose was tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person.

390. Consumers have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused third-party Pixels and cookies (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiffs' and Class members' computing devices as "first-party" cookies that are not blocked.

391. Defendant's scheme or artifice to defraud in this action consists of:

- a. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited in the claims below;
- b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Facebook.

392. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and Class Members' property:

- a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and
- b. property rights to determine who has access to their computing devices.

393. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and Class Members' property:

- a. with knowledge that (1) Defendant did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Facebook was collecting their Private Information based on their activities on Defendant's Website; (4) "a reasonable Facebook user would be shocked to realize" the extent of Facebook's collection of Private Information; (5) a Covered Incident had occurred which required a report to be made to the FTC pursuant to Facebook's consent decrees with the FTC and (6) the subsequent use of health information for advertising was a further invasion of such property rights in making their own exclusive use of their Private Information for any purpose not related to the provision of their healthcare; and
- b. with the intent to (1) acquire Plaintiffs and Class Members' Private Information without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use Plaintiffs' and Class Members' Private

Information without their authorization and (3) gain access to Plaintiffs' and Class Members' personal computing devices through the 'fbp' cookie disguised as a first-party cookie.

394. As a direct and proximate result of Defendant's violation of the ECPA, Plaintiffs and Class Members were damaged by Defendant's conduct and Defendant is liable to Plaintiffs and Class Members for violations of the ECPA.

395. Based on the foregoing, Plaintiff and Nationwide Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

COUNT II

NEGLIGENCE

(On behalf of Plaintiffs & the Nationwide Class)

396. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

397. Upon accepting, storing, and controlling the Private Information of Plaintiffs and the Class, Defendant owed, and continues to owe, a duty to Plaintiffs and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information.

398. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information from unauthorized disclosure.

399. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information through their use of the Pixels and other tracking technologies would result in unauthorized third parties, such as Facebook and/or Google, gaining access to such Private Information for no lawful purpose.

400. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiffs' and Class members' Private Information arose due to the special relationship that existed between Defendant and their patients, which is recognized by statute, regulations, and the common law.

401. In addition, Defendant had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation. As alleged herein, Defendant also had a duty under the FTCA not to engage in unfair business practices by sharing patient data without informed consent. Further, as Aspen treats patients as young as six years old, it had an additional duty to obtain parental consent before sharing any patients under the age of 13, pursuant to the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6505.

402. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendant's misconduct included the failure to (1) secure Plaintiffs' and Class members' Private Information; (2) comply with industry-standard data security practices; (3) implement adequate website and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Pixels and other tracking technologies.

403. As a direct result of Defendant's breach of their duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' Private Information, Plaintiffs and the Class

have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

404. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiffs' and Class members' Private Information constituted (and continue to constitute) negligence at common law.

405. Plaintiffs and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT III

INVASION OF PRIVACY

(On behalf of Plaintiffs & the Nationwide Class)

406. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

407. The highly sensitive and personal Private Information of Plaintiffs and Class members consists of private and confidential facts and information regarding Plaintiffs' and Class members' health that were never intended to be shared beyond private communications on the Website and the consideration of health professionals.

408. Plaintiffs and Class members had a reasonable and legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this Information against disclosure to unauthorized third parties, including Facebook and/or Google.

409. Defendant owed a duty to Plaintiffs and Class members to keep their Private Information confidential.

410. Defendant's unauthorized disclosure of Plaintiffs' and Class members' Private Information to Facebook and/or Google or any other third-party tech and marketing giants is highly offensive to a reasonable person.

411. Defendant's willful and intentional disclosure of Plaintiffs' and Class members' Private Information constitutes an intentional interference with Plaintiffs' and Class members' interest in solitude and/or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

412. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class members' privacy because Defendant facilitated Facebook's and/or Google's simultaneous eavesdropping and wiretapping of confidential communications.

413. Defendant failed to protect Plaintiffs' and Class members' Private Information and acted knowingly when they installed the Pixels onto the Website because the purpose of the Pixels is to track and disseminate individual's communications on the Website for the purpose of marketing and advertising.

414. Because Defendant intentionally and willfully incorporated the Pixels into the Website and encouraged individuals to use and interact with the Website and the health services thereon, Defendant had notice and knew that their practices would cause injury to Plaintiffs and the Class.

415. There is no legitimate public concern with respect to the Private Information of Plaintiffs and Class Members.

416. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information, including the PII and PHI of Plaintiffs and Class members, was disclosed to

unauthorized third parties including Facebook and/or Google causing Plaintiffs and the Class to suffer damages.

417. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, lost benefit of the bargain, plus pre-judgment interest and costs.

418. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendant and still in the possession of Facebook, Google, and other unauthorized third parties, and the wrongful disclosure of the Private Information cannot be undone.

419. Plaintiffs and Class members have no adequate remedy at law for the injuries relating to Defendant's and unauthorized third parties' continued possession of their sensitive and confidential Private Information. A judgment for monetary damages will not undo Defendant's disclosure of the Private Information to unauthorized third parties who, upon information and belief, continue to possess and utilize the Private Information.

420. Plaintiffs, on behalf of themselves and Class members, further seek injunctive relief to enjoin Defendant from intruding into the privacy and confidentiality of Plaintiffs' and Class members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

421. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT IV

UNJUST ENRICHMENT

(On behalf of Plaintiffs & the Nationwide Class)

422. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein. This count is pleaded in the alternative to breach of implied contract.

423. Defendant benefits from the use of Plaintiffs' and Class members' Private Information and unjustly retained those benefits at Plaintiffs' and Class members' expense.

424. Plaintiffs and Class members conferred a benefit upon Defendant in the form of the monetizable Private Information that Defendant collected from them and disclosed to third parties, including Facebook and/or Google, without authorization and proper compensation.

425. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

426. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class members because Defendant's conduct damaged Plaintiffs and Class members, all without providing any commensurate compensation to Plaintiffs or Class members.

427. The benefits that Defendant derived from Plaintiffs and Class members were not offered by Plaintiffs or Class members gratuitously and, thus, rightly belongs to Plaintiffs and Class members. It would be inequitable under unjust enrichment principles in Massachusetts and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

428. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT V

BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs & the Nationwide Class)

429. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein. This count is pleaded in the alternative to unjust enrichment.

430. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information through Defendant's Site as part of its regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

431. Defendant required Plaintiffs and Class Members to provide their Private Information, including full names, email addresses, phone numbers, computer IP addresses, appointment information, medical insurance information, medical provider information, medical histories, and other content submitted on Defendant's Site as a condition of their receiving healthcare services.

432. As a condition of utilizing Defendant's Site and receiving services from Defendant, Plaintiffs and Class Members provided their Private Information and compensation for their medical care. In so doing, Plaintiffs and Class Members entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

433. Implicit in the agreement between Defendant and its patients was the obligation that both parties would maintain the Private Information confidentially and securely.

434. Defendant had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in its possession was used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Defendant.

435. Defendant had an implied duty to protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses.

436. Additionally, Defendant implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

437. Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

438. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant. Defendant did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information for uses other than medical treatment, billing, and benefits from Defendant.

439. Consumers of medical services value their privacy and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, nor would Plaintiffs and Class Members have entrusted their Private Information to Defendant in the absence of Defendant's implied promise to monitor the Site,

computer systems, and networks to ensure that reasonable data security measures were adopted and maintained.

440. Defendant breached the implied contracts with Plaintiffs and Class Members by disclosing Plaintiffs' and Class Members' Private Information to unauthorized third parties, failing to properly safeguard and protect Plaintiffs' and Class Members' Private Information; and violating industry standards as well as legal obligations that are necessarily incorporated into implied contract between Plaintiffs, Class Members, and Defendant.

441. The Disclosure was a reasonably foreseeable consequence of Defendant's actions in breach of the implied contracts.

442. Defendant's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class Members to provide their Personal Information in exchange for medical treatment and benefits.

443. As a result of Defendant's failure to fulfill the data security protections promised in these implied contracts, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value.

444. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities, the loss of control of their Private Information, disruption of their medical care and treatment, and the loss of the benefit of the bargain they had struck with Defendant.

445. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT VI

**VIOLATIONS OF ILLINOIS CONSUMER FRAUD
AND DECEPTIVE BUSINESS PRACTICES ACT**

815 Ill. Comp. Stat. 505/1, *et seq.*

(On behalf of Plaintiffs A.D., C.A., R.G., & the Illinois Subclass)

446. Plaintiffs A.D., C.A., and R.G. re-allege and incorporate by reference the allegations above as if fully set forth herein.

447. Defendant is a “person” as defined by 815 ILCS § 505/1.

448. Plaintiffs and Illinois Subclass Members are “consumers” as defined by 815 ILCS § 505/1.

449. Defendant’s unfair acts and practices against Plaintiffs and Illinois Subclass Members occurred in the course of trade or commerce in Illinois, arose out of transactions that occurred in Illinois, and/or harmed individuals in Illinois.

450. Plaintiffs and Illinois Subclass Members received and paid for health care services from Defendant.

451. Plaintiffs and Illinois Subclass Members used Defendant’s Website from Illinois.

452. Plaintiffs’ and Illinois Subclass Members’ payments to Defendant for health care services were for household and personal purposes.

453. Defendant’s practices of disclosing Plaintiffs’ and Illinois Subclass Members’ PII and PHI by re-directing confidential communications via the Pixel to third parties without authorization, consent, or knowledge of Plaintiffs and Illinois Subclass Members is a deceptive, unfair, and unlawful trade act or practice, in violation of 815 ILCS § 505/2.

454. Defendant’s unfair business practices were targeted at all of Defendant’s Users, including Plaintiffs and Illinois Subclass Members.

455. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the privacy, security, and use of their personally identifiable patient data and communications when using Defendant's Website.

456. Defendant intended to mislead Plaintiffs and Illinois Subclass Members and to induce them to rely on its misrepresentations and omissions.

457. Defendant's surreptitious collection and disclosure of Plaintiffs' and Illinois Subclass Members' PII, PHI, and communications to third parties involves important consumer protection concerns.

458. Furthermore, the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/20, provides that a violation of that statute constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 et seq. ("ICFA").

459. Defendant is a "data collector" under IPIPA.¹¹⁰ As a data collector, Defendant owns or licenses information concerning Illinois residents.

460. IPIPA protects Medical Information and Personal Information.¹¹¹

461. The IPIPA requires a data collector that "maintains or stores . . . records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."¹¹²

¹¹⁰ 815 ILL. COMP. STAT. 530/5.

¹¹¹ *Id.*

¹¹² 815 ILL. COMP. STAT. 530/45(a).

462. IPIPA's rights are not subject to waiver.¹¹³

463. Defendant represented that it would safeguard and protect Plaintiffs' and Illinois Subclass Members' Private Information, in its Privacy Policy and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Illinois Subclass Members if their data had been breached and compromised or stolen.

464. Defendant made these representations with the intent to induce Plaintiffs and Illinois Subclass Members to seek health care services from Defendant and to use Defendant's Website in doing so.

465. Plaintiffs and Illinois Subclass Members relied upon Defendant's representations in seeking health care services from Defendant and in using Defendant's Website to obtain such services.

466. The IPIPA further requires that data collectors "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most *expedient* time possible and *without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system."¹¹⁴

467. As alleged above, Defendant violated the IPIPA by failing to implement and maintain reasonable security measures to protect Plaintiffs and Illinois Subclass Members' PHI and PII. Defendant further violated the IPIPA by failing to give Plaintiffs and Illinois Subclass Members expedient notice without unreasonable delay.

¹¹³ 815 ILL. COMP. STAT. 530/15.

¹¹⁴ 815 ILL. COMP. STAT. 530/10 (emphasis added).

468. As a direct and proximate cause of Defendant's unfair acts and practices, Plaintiffs and Illinois Subclass Members have suffered actual damages.

469. Plaintiffs' and Illinois Subclass Members' injuries were proximately caused by Defendant's unfair and deceptive business practices.

470. As a result of Defendant's conduct, Defendant has been unjustly enriched.

471. Defendant's acts caused substantial injury that Plaintiffs and Illinois Subclass Members could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

472. Defendant acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiffs' and Illinois Subclass Members' rights.

473. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including overpaying for Defendant's health care services and loss of value of their personally identifiable patient data and communications.

474. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass Members were also damaged by Defendant's conduct in that:

- a. Defendant harmed Plaintiffs' and Illinois Subclass Members' interest in privacy;
- b. Sensitive and confidential information that Plaintiffs and Illinois Subclass Members intended to remain private has been disclosed to third parties;

- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. Defendant took something of value from Plaintiffs and Illinois Subclass Members, *i.e.*, their personally identifiable patient information, and derived a benefit therefrom without Plaintiffs' or Illinois Subclass Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;
- e. Plaintiffs and Illinois Subclass Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality and
- f. Defendant's actions diminished the value of Plaintiffs' and Illinois Subclass Members' personal information.

475. As a direct and proximate result of Defendant's above-described violation of the IPIPA and ICFA, Plaintiffs A.D., C.A., and R.G. and Illinois Subclass Members are entitled to recover actual damages, reasonable attorneys' fees, and costs.

COUNT VII

VIOLATION OF ILLINOIS EAVESDROPPING STATUTE 720 Ill. Comp. Stat. 5/14, *et seq.* (*On Behalf of Plaintiffs A.D., C.A., and R.G. & the Illinois Subclass*)

476. Plaintiffs A.D., C.A., and R.G. re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

477. The Eavesdropping Article of the Illinois Criminal Code (the "Illinois Eavesdropping Statute" or "IES") states that it is a felony for any person to knowingly and intentionally "use[] an eavesdropping devise, in a surreptitious manner, for the purpose of transmitting or recording all or part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation."¹¹⁵

¹¹⁵ 720 ILL. COMP. STAT. 5/14-2(a), -4.

478. The IES also states that it is a felony for any person to knowingly and intentionally “use[] or disclose[] any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of this Article, unless he or she does so with the consent of all of the parties.”¹¹⁶

479. For purposes of the IES, “eavesdropping device” means “any device capable of being used to hear or record oral conversation or intercept or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means.”¹¹⁷

480. For purposes of the IES, “surreptitious” means “obtained or made by stealth or deception, or executed through secrecy or concealment.”¹¹⁸

481. For purposes of the IES, “private electronic communication” means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. . . . Electronic communication does include any communication from a tracking device.”¹¹⁹

¹¹⁶ *Id.*

¹¹⁷ 720 ILL. COMP. STAT. 5/14-1(a).

¹¹⁸ 720 ILL. COMP. STAT. 5/14-1(g).

¹¹⁹ 720 ILL. COMP. STAT. 5/14-1(e).

482. “A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution.”¹²⁰

483. Defendant intentionally recorded and/or acquired Plaintiffs’ and Illinois Subclass Members’ private electronic communications in Illinois, without the consent of Plaintiffs and Illinois Subclass Members, using the Pixels, Google Analytics and similar tracking technologies on its Website.

484. Defendant intentionally recorded and/or acquired Plaintiffs’ and Illinois Subclass Members’ private electronic communications for the purpose of disclosing those communications to third parties, including Facebook and Google, without the knowledge, consent, or written authorization of Plaintiffs or Illinois Subclass Members.

485. Plaintiffs’ and Illinois Subclass Members’ communications with Defendant which took place in Illinois, constitute private conversations, communications, and information.

486. Plaintiffs and Illinois Subclass Members had a reasonable expectation of privacy in their communications with Defendant via its Website.

487. Plaintiffs and Illinois Subclass Members communicated sensitive PHI and PII that they intended for only Defendant to receive and that they understood Defendant would keep private.

488. Plaintiffs and Illinois Subclass Members have a reasonable expectation that Defendant would not disclose PII, PHI, and confidential communications to third parties without Plaintiffs’ or Illinois Subclass Members’ authorization, consent, or knowledge.

¹²⁰ *Id.*

489. Plaintiffs and Illinois Subclass Members had a reasonable expectation of privacy given Defendant's representations, Privacy Policy and HIPAA. Moreover, Plaintiffs and Illinois Subclass Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

490. Plaintiffs and Illinois Subclass Members were unaware that their Private Information was being surreptitiously recorded and transmitted to third parties such as Facebook and/or Google as they communicated with Defendant through its Website.

491. Without Plaintiffs' or Illinois Subclass Members' knowledge, authorization, or consent, Defendant used the Meta Pixel, Google Analytics and other tracking codes imbedded and concealed into the source code of its Website, to secretly record and transmit Plaintiffs' and Illinois Subclass Members' private communications to hidden third parties, such as Facebook and Google.

492. Under the IES, "[a]ny or all parties to any conversation or electronic communication upon which eavesdropping is practiced contrary to this Article shall be entitled to the following remedies: (a) [t]o an injunction by the circuit court prohibiting further eavesdropping by the eavesdropper and by or on behalf of his principal, or either; (b) [t]o all actual damages against the eavesdropper or his principal or both; [t]o any punitive damages which may be awarded by the court or by a jury. . . ." ¹²¹

493. The eavesdropping devices used in this case include, but are not limited to:

- a. The Pixels, Google Analytics, cookies and other third party tracking codes and programs employed by Defendant on its Website;
- b. Plaintiffs' and Illinois Subclass Members' personal computing devices;
- c. Plaintiffs' and Illinois Subclass Members' web browsers;
- d. Plaintiffs' and Illinois Subclass Members' browser-managed files;
- e. Defendant's web servers; and

¹²¹ 720 ILL. COMP. STAT. 5/14-6.

- f. Web and ad-servers of third parties (including Facebook and/or Google) to which Plaintiffs' and Illinois Subclass Members' communications were disclosed.

494. The eavesdropping devices outlined above are not excluded "tracking devices" as that term is used in the IES, 720 ILCS 5/14-1(e), to the extent that they perform functions other than collection of geo-locational data.¹²²

495. Defendant is a "person" under the IES.¹²³

496. Defendant aided in the interception of communications between Plaintiffs and Illinois Subclass Members and Defendant that were redirected to and recorded by third parties without Plaintiffs' or Illinois Subclass Members' consent.

497. Under the IES, Plaintiffs and Illinois Subclass Members are entitled to injunctive relief prohibiting further eavesdropping by Defendant, actual damages, and punitive damages.

498. Defendant's breach caused Plaintiffs and Illinois Subclass Members the following damages:

- a. Sensitive and confidential information that Plaintiffs and Illinois Subclass Members intended to remain private is no longer private;
- b. Defendant eroded the essential confidential nature of the physician-patient relationship;
- c. Defendant took something of value from Plaintiffs and Illinois Subclass Members and derived benefit therefrom without Plaintiffs' and Illinois Subclass Members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiffs and Illinois Subclass Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality and

¹²² See *Vasil v. Kiip, Inc.*, No. 16-cv-9937, 2018 U.S. Dist. LEXIS 35573, at *20-25 (N.D. Ill. Mar. 5, 2018).

¹²³ 720 ILL. COMP. STAT. 5/2-15.

- e. Defendant's actions diminished the value of Plaintiffs' and Illinois Subclass Members' personal information.

499. Plaintiffs A.D., C.A., and R.G. and Illinois Subclass Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT VIII

VIOLATION OF THE FLORIDA SECURITY OF COMMUNICATIONS ACT

Fla. Stat. § 934.01, *et seq.*

(On behalf of Plaintiff M.H. & the Florida Subclass)

500. Plaintiff M.H. re-alleges and incorporates the foregoing allegations above as if fully set forth herein.

501. The Florida Secretary of Communications Act ("FSCA") is codified at Florida Statutes, § 934.01, *et seq.* The FSCA begins with legislative findings, including:

On the basis of its own investigations and of published studies, the Legislature makes the following findings...(4) to safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communications has consented to the interceptions should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court.

502. Florida Statutes § 934.10 provides, in pertinent part, as follows:

Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of §§ 934.04-934.09 shall have a civil cause of action against any person or entity who intercepts, discloses, or uses, or procures any person or entity to intercept, disclose, or use, such communications and shall be entitled to recover from any such person or entity which engaged in that violation such relief as may be appropriate, including: (a) [p]reliminary or equitable declaratory relief as may be appropriate; (b) [a]ctual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of the violation or \$1,0000, whichever is higher; (c) [p]unitive damages; and (d) [a] reasonable attorney's fee and other litigation costs reasonably incurred.

503. The FCSA defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical systems that affects intrastate, interstate, or foreign commerce.” Fla. Stat. § 934.02(12).

504. It further defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Fla. Stat. § 934.02(3).

505. At all relevant times, Defendant aided, employed, agreed with, and conspired with Facebook to intercept Plaintiff’s and the Florida Subclass Members’ internet communications in Florida while accessing <https://www.aspendental.com>, including the contents thereof—*i.e.*, the URLs visited, the medical dental conditions and types of treatments searched, and appointment details. Such information not only constitutes protected health information, but it also represents the substance, import, and meaning of the communications between Plaintiff and other Florida Subclass Members had with Defendant’s Website.

506. Plaintiff M.H. and other Florida Subclass Members had a reasonable expectation of privacy in the electronic communications they had with Defendant’s Website.

507. Nonetheless, these electronic communications were transmitted to and intercepted by a third party (*i.e.*, Facebook) during the communication and without knowledge, authorization, or consent of Plaintiff and Florida Subclass Members. That is because Defendant intentionally inserted an electronic device into its Website that, without the knowledge and consent of Plaintiff and Florida Subclass Members, recorded and transmitted the substance of their confidential communications with Defendant to a third party.

508. Plaintiff M.H. and other members of the Florida Subclass used Defendant's Website from Florida.

509. Defendant willingly facilitated Facebook's interception and collection of Plaintiff's and Florida Subclass Members' Private Information by embedding the Meta Pixel and other third party tracking codes on its Website.

510. Defendant used the following items as a device or apparatus to intercept wire, electronic, or oral communications made by Plaintiff and other Class Members:

- a. The Pixels, Google Analytics, cookies and other tracking codes and programs deployed by Defendant to track Plaintiff's and Florida Subclass Members' communications while they were navigating Defendant's Website;
- b. Plaintiff's and Florida Subclass Members' browsers;
- c. Plaintiff's and Florida Subclass Members' computing and mobile devices;
- d. Defendant's web and ad-servers;
- e. The web and ad-servers from which Facebook tracked and intercepted Plaintiff's and Florida Subclass Members' communications while they accessed and/or navigated Defendant's Website, and
- f. The Pixels, Google Analytics, cookies and other computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiff's and Florida Subclass Members' communications while they used Defendant's Website.

511. Defendant fails to disclose that it is using the Meta Pixel specifically (and other invisible tracking technologies from third parties) to track and automatically and simultaneously transmit communications to a third party, *i.e.*, Facebook.

512. To avoid liability under the FCSA, a defendant must show it had the consent of all parties to a communication.

513. The patient communication information that Defendant transmits to Facebook and other unauthorized third parties while using the Meta Pixel and other tracking codes, such as doctor

appointment booking information and Users' names, email addresses, IP addresses, unique personal identifiers such as the FID and home addresses, constitutes protected health information.

514. As demonstrated hereinabove, Defendant violates the FCRA by aiding and permitting third parties such as Facebook to receive its Users' online communications in real time through its Website without their consent.

COUNT IX

VIOLATION OF THE MASSACHUSETTS CONSUMER PROTECTION ACT

M.G.L. § 93A, *et seq.*

(On behalf of Plaintiff S.B. & the Massachusetts Subclass)

515. Plaintiff S.B. re-alleges and incorporates the foregoing allegations above as if fully set forth herein.

516. The Massachusetts Consumer Protection Act, M.G.L. c. 93A *et seq.* prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of Massachusetts.

517. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of M.G.L. c. 93A. Defendant's conduct alleged herein is a "business practice" within the meaning of M.G.L. c. 93A, and the deception occurred within the commonwealth of Massachusetts.

518. Plaintiff S.B. and other members of the Massachusetts Subclass used Defendant's Website from Massachusetts. Their Private Information was collected and transmitted by operation of the Pixels and/or Google Analytics, which were instantiated in the Source Code running in their browser or mobile application.

519. Defendant solicited, obtained, and stored Plaintiff S.B.'s and Massachusetts Subclass' Private Information and knew or should have known not to disclose such Private Information to Facebook, Google and other unauthorized third parties through use of the Pixels

and other tracking technologies.

520. Plaintiff S.B. and Massachusetts Subclass Members would not have provided their Private Information if they had been told or knew that Defendant would be disclosing such information to Facebook, Google and other unauthorized third parties.

521. As alleged herein, Defendant engaged in the unfair or deceptive acts or practices in the conduct of consumer transactions in violation of M.G.L. c. 93A, including but not limited to:

- a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;
- b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff S.B.'s and Massachusetts Subclass Members' Private Information from unauthorized disclosure;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff S.B.'s and Massachusetts Subclass Members' Private Information, including duties imposed by Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data, HIPAA, and COPPA, 15 U.S.C. §§ 6501-6505. Defendant's failure was a direct and proximate cause of the unauthorized disclosure of Plaintiff S.B.'s and Massachusetts Subclass Members' Private Information;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff S.B.'s and Massachusetts Subclass Members' Private Information from unauthorized disclosure;
- e. Omitting, suppressing, and concealing the material fact that it did not intend to protect Plaintiff S.B.'s and Massachusetts Subclass Members' Private Information from unauthorized disclosure, and
- f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff S.B.'s and Massachusetts Subclass Members' Personal Information, including duties imposed by the FTCA, HIPAA, and COPPA, which failure was a direct and proximate cause of the unauthorized disclosure.

522. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to

protect the confidentiality of consumers' Private Information.

523. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer by providing his or her Private Information to Defendant. The requests for and use of such Private Information in Massachusetts through deceptive means were consumer-oriented acts and thereby fall under the Massachusetts Consumer Protection Act.

524. In addition, Defendant's failure to secure its Users' Private Information violated the FTCA and therefore violated the Massachusetts Consumer Protection Act.

525. Defendant knew or should have known that its computer systems and data security practices—in particular, its use of the Pixels, Conversions API and/or Google Analytics—were inadequate to safeguard the Private Information of Plaintiff and Massachusetts Subclass Members, and that enabling third parties to collect the Private Information of Plaintiff and the Massachusetts Subclass constituted a data breach.

526. Defendant's violations of the Massachusetts Consumer Protection Act have an impact and general importance to the public, including the people of this commonwealth. Thousands of Massachusetts citizens have had their Private Information transmitted without consent from Defendant's Website to third parties.

527. Defendant's implied and express representations that it would adequately safeguard Plaintiff S.B.'s and Massachusetts Subclass Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of the Massachusetts Consumer Protection Act.

528. As a direct and proximate result of these deceptive trade practices, Plaintiff S.B. and Class Members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Massachusetts legislature.

529. Accordingly, Plaintiff S.B., on behalf of themselves and Massachusetts Subclass

Members, brings this action under M.G.L. c. 93A to seek such injunctive relief necessary to enjoin further violations, to recover actual damages, treble damages, the costs of this action (including reasonable attorneys' fees and costs), and such other relief as the Court deems just and proper.

COUNT X

VIOLATION OF THE MASSACHUSETTS WIRETAP ACT

M.G.L. c. 272 § 99

(On behalf of Plaintiff S.B. & the Massachusetts Subclass)

530. Plaintiff S.B. re-alleges and incorporates the foregoing allegations above as if fully set forth herein.

531. The Massachusetts Wiretap Act, M. G. L. c. 272 § 99 makes it an unlawful act to “secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication.” *Id.* ¶ (B)(4), (C). The Act provides a private remedy to any “person whose oral or wire communications were intercepted.” *Id.* ¶ (C).

532. An individual’s communications with a website constitute “wire communications” as defined in the Massachusetts Wiretap Act, M.G.L. c. 272 § 99(B)(1). The communications between Plaintiff and other Massachusetts Subclass Members and Defendant, through the Defendant’s Website, were therefore wire communications under the Massachusetts Wiretap Act.

533. The tracking technologies inserted into the hidden code of the Defendant’s Website, including the Pixels, Conversions API, and Google Analytics, are “intercepting devices” as defined in the Massachusetts Wiretap Act, M.G.L. c. 272 § 99(B)(3). “Intercepting devices” also include (i) any devices Massachusetts Subclass Members used to access Defendant’s Website; (ii)

Massachusetts Subclass Members' web browsers used to access Defendant's Website; (iii) Defendant own computer servers; and (iv) the computer servers of third parties such as Facebook and Google which intercepted Plaintiff's and Massachusetts Subclass Members' communications with the Defendant's Website.

534. The computer code for tracking technologies such as the Pixels and Google Analytics, and others enabled Facebook, Google and other third parties to record and disclose to Facebook, Google and other third parties the contents of communications between Defendant and Users of the Defendant's Website, including, but not limited to, the identity of the parties to the communication, the existence of the communication, and the communication's content, substance, purport, and meaning, including but not limited to (i) the identity of webpages the user visited; (ii) their medical dental conditions and specific treatments sought; and (iii) details of their dental appointments.

535. By inserting the computer code for the Meta Pixel, Google Analytics, and other tracking technologies, Defendant installed an intercepting device on its Website with the intent to aid Facebook, Google and likely other unauthorized third parties to secretly hear and record communications between Plaintiff, the Massachusetts Subclass Members and Defendant.

536. Plaintiff's and Massachusetts Subclass Members' communications with Defendant were intercepted, disclosed to Facebook as well as other third parties, and used without their knowledge or consent. Moreover, their privacy interests were violated by the interception.

537. Plaintiff S.B. and other members of the Massachusetts Subclass used Defendant's Website from Massachusetts.

538. Pursuant to the Massachusetts Wiretap Act, Plaintiff S.B. seeks for themselves and each Massachusetts Subclass Member statutory damages of \$100 for each day of Defendant's

violation of the Massachusetts Wiretap Act for Plaintiff and each Massachusetts Subclass Member, or \$1,000 with respect to the Plaintiff S.B. and each Massachusetts Subclass Member, whichever is higher, plus reasonable attorneys' fees and other litigation disbursements that their counsel has incurred and will reasonably incur in prosecuting this action.

COUNT XI

VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT

Wash. Rev. Code Ann. §§ 19.86.020, *et seq.*

(On Behalf of Plaintiff E.W. and the Washington Subclass)

539. Plaintiff E.W. repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

540. Defendant is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

541. Defendant advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

542. Defendant engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

- a. Failing to secure and protect Plaintiff's and Washington Subclass Members' Private Information in a confidential manner;
- b. Failing to inform Plaintiff and Washington Subclass Members of Defendant's use of the Meta Pixel, Conversions API, Google Analytics, and other tracking tools;
- c. Failing to inform Plaintiff and Washington Subclass Members of the extent of Defendant's data harvesting, tracking, and disclosure practices;
- d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the unauthorized disclosure of their Private Information;

- e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Washington Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- g. Misrepresenting that certain sensitive Private Information would not be disclosed to third parties;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Washington Subclass Members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

543. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's ability and intentions to

protect the confidential and sensitive Private Information of Plaintiff and Washington Subclass Members communicated for the purpose of medical treatment.

544. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Washington Subclass Members, that their Private Information would be held in a secure and confidential manner, rather than deliberately disclosed to third parties.

545. Defendant acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass Members' rights.

546. Defendant's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, including, but not limited to Wash. Rev. Code §§ 19.255.010, et seq.. Alternatively, Defendant's conduct is injurious to the public interest because it has injured Plaintiff and Washington Subclass Members, had the capacity to injure persons, and has the capacity to injure other persons, and has the capacity to injure persons. Further, its conduct affected the public interest, including the thousands of Washington Residents impacted by Defendant's use of the Meta Pixel, Conversions API, Google Analytics, and other tracking tools.

547. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including the damage to their privacy and property interests in their Private Information.

548. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

COUNT XII

VIOLATION OF THE WASHINGTON HEALTH CARE INFORMATION ACT RCW 70.2.005, et seq. (On Behalf of Plaintiff E.W. and the Washington Subclass)

549. Plaintiff E.W. repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

550. The Washington HCIA, RCW 70.2.005, et seq., states that “a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient’s written authorization.”

551. The HCIA defines “health care information” to mean “any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient’s health care” RCW 70.02.010(17).

552. Defendant is a health care facility as defined by RCW 70.010(16).

553. By deploying code on its website to capture and transmit its patients’ personally identifiable and health information to third parties, Defendant discloses Plaintiff’s and Washington Subclass members’ health care information without their written authorization.

554. As a direct and proximate cause of Defendant’s actions, Plaintiff and Washington Subclass members were damaged in that:

- a. Sensitive, confidential, and/or protected information that Plaintiff and Washington Subclass members intended to remain private is no more;
- b. Defendant took something of value from Plaintiff and Washington Subclass members and derived benefit therefrom without Plaintiff's and Washington Subclass members' knowledge or informed consent and without sharing the benefit of such value;
- c. Plaintiff and Washington Subclass members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality of patient data and communications; and
- d. Defendant's actions diminished the value of Plaintiff's and Washington Subclass members' personally identifiable patient data and communications.

555. Plaintiff and Washington Subclass members seek an order requiring Defendant to comply with the HCIA, actual damages, and attorneys' fees and costs.

COUNT XIII

IDENTITY THEFT IN VIOLATION OF RCW 9.35.020 (On Behalf of Plaintiff E.W. and the Washington Subclass)

556. Plaintiff E.W. repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

557. RCW 9.35.020 states: "No person may knowingly obtain, possess, use, or transfer a means of identification or financial information of another person, living or dead, with the intent to commit, or to aid or abet, any crime."

558. Under RCW 9.35.005, "means of identification" connotes, among other things, "information or an item that is not describing finances or credit but is personal to or identifiable

with an individual or other person, including: A current or former name of the person, ... an electronic address, or identifier of the individual or a member of his or her family, ... and other information that could be used to identify the person”

559. Defendant is a “person” as defined by RCW 9A.04.110(17).

560. The IP addresses, cookie identifiers, and browser fingerprint information used and transferred by Defendant constitute “means of identification” because they include electronic addresses and identifiers and information that could be used to identify Plaintiff and Washington Subclass members.

561. By deploying source code at the Website that captures and transmits patients’ personally identifiable information and communications to third parties without patients’ authorization, Defendant knowingly obtains, possesses, uses, and/or transfers Plaintiff’s and Washington Subclass members’ means of identification, including electronic addresses and other identifiers, with the intent to aid and abet third parties’ violations of the Washington Privacy Act, RCW 9.73.030.

562. The Washington Privacy Act makes it unlawful to “intercept or record, any ... [p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by device, electronic or otherwise, designed to record and/or transmit said communication, regardless of how such device is powered or actuated, without first obtaining the consent of all the participants in the communication.”

563. Communications between Plaintiff and Washington Subclass members and Defendant, including Plaintiff’s and Washington Subclass members’ identities and the content of their communications with Defendant, constitute private communications transmitted by an electronic device “designed to record and/or transmit said communications.”

564. The third parties intercept and record Plaintiff's and Washington Subclass members' communications by redirecting the contents of Plaintiff's and Washington Subclass members' communications from their personal computers, web browsers, and browser-managed files, Internet cookies, and Defendant's computer servers to their own servers using computer code the third parties provided to Defendant.

565. As a direct and proximate cause of Defendant's actions, Plaintiff and Washington Subclass members were damaged in that:

- a. Sensitive, confidential, and/or protected information that Plaintiff and Washington Subclass members intended to remain private is no more;
- b. Defendant took something of value from Plaintiff and Washington Subclass members and derived benefit therefrom without Plaintiff and Washington Subclass members' knowledge or informed consent and without sharing the benefit of such value;
- c. Plaintiff and Washington Subclass members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality of patient data and communications; and
- d. Defendant's actions diminished the value of Plaintiff's and Washington Subclass members' personally identifiable patient data and communications.

566. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including statutory damages under RCW 9.35.020(7), actual damages, injunctive relief, and other appropriate equitable relief, as well as attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class and the

Subclasses, respectfully request that this Court enter an Order:

- a) Certifying this case as a class action on behalf of the Nationwide Class and Subclasses defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as Class Counsel;
- b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or unauthorized disclosure of Plaintiffs' and Class members' Private Information;
- c) For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members;
- d) For an award of damages, including but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;
- e) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- f) Pre- and post-judgment interest on any amounts awarded and
- g) Such other and further relief as this Court may deem just and proper.

Date: February 20, 2024

Respectfully submitted,

By: /s/ Brandon M. Wise

Brandon M. Wise – IL Bar # 6319580
PEIFFER WOLF
CARR KANE CONWAY & WISE, LLP
One U.S. Bank Plaza, Suite 1950
St. Louis, MO 63101
Ph: (314) 833-4825
bwise@peifferwolf.com

Andrew R. Tate – GA Bar #518068*
PEIFFER WOLF
CARR KANE CONWAY & WISE, LLP
235 Peachtree Street NE, Suite 400
Atlanta, GA 30303
Ph: (404) 282-4806

atate@peifferwolf.com

*Pro Hac Vice To Be Filed

Attorneys for Plaintiffs & Putative Classes